ENDPOINT PROTECTOR

User Manual Version 4.4.0.4

User Manual

COSOSYS

Table of Contents

1. Introduction 1
   1.1. What is Endpoint Protector? 2
   1.2. Main Features 4
      1.2.1. Centralized web based Device Management / Dashboard 4
      1.2.2. Control your data flow: File Tracing / File Shadowing 4
      1.2.3. Audit Trail – Device Activity Logging 5
      1.2.4. Audit Trail – Reporting and Analysis Tools 5
      1.2.5. Sensitive Content Filtering 5
      1.2.6. File Whitelist 5
      1.2.7. Easy Enforcement of Your Security Policies 5
      1.2.8. Network "Offline" Mode to Support Your Field Employees 5
      1.2.9. Enforced Encryption - protecting sensitive data in transit / Trusted Device 6
      1.2.10. Client Uninstall Protection 6
      1.2.11. Client Stop Protection / Tamper Protection 6
      1.2.12. Backup Scheduler 6
   1.3. Controlled Device Types / Ports 7
   1.4. Conclusions 9
2. Server Functionality / Server Components 10
   2.1. Endpoint Protector – Web Service 11
   2.2. Administration and Reporting Tool 11
   2.3. Accessing the Administration and Reporting Tool 14
   2.4. Login Credentials (Username and Password) 15
   2.5. General Dashboard 15
   2.6. System Status 16
   2.7. Live Update 17
3. Endpoint Management 19
   3.1. Devices 19
   3.2. Device Functionality 20
      3.2.1. Give / Deny Access to Devices 21
      3.2.2. Enable Device Read-Only Access 23
      3.2.3. TrustedDevice Level 1 to Level 4 23

3.2.4. WiFi - Block if wired network is present 23
3.3. Computers 24
3.4. Groups 25
3.5. Users 26
3.6. Custom Classes 27
4. Endpoint Rights 29
4.1. Device Rights 30
4.2. User Rights 31
4.3. Computer Rights 32
4.4. Group Rights 33
4.5. Global Rights 34
4.6. Effective Rights 35
4.6.1. Effective Rights for Endpoints 35
4.6.2. Effective Rights for Devices 35
4.6.3. Effective Rights for Content Aware Protection 36
4.7. File Whitelist 36
5. Offline Temporary Password 38
5.1. Generating the Offline Temporary Password 38
5.2. Device Offline Temporary Password 39
5.3. Computer Offline Temporary Password 41
5.4. Content Aware Protection Offline Temporary Password 41
5.5. Offline Device, Computer and Content Aware Protection Authorization 42
5.6. Setting the Administrator Contact Information 43
6. Endpoint Settings 44
6.1. Computer Settings 47
6.2. Group Settings 48
6.3. Global Settings 49
6.4. Custom Client Notifications 50
6.5. File Tracing 53
6.6. File Shadowing 54

6.7. CAP File Shadowing 56
6.8. Network Share Tracing 57
7. Content Aware Protection 59
7.1. Activation of Content Aware Protection 60
7.2. Content Aware Policies 61
7.2.1. Priorities for Content Aware Policies 62
7.2.2. How Content Aware Policies Work 62
7.2.3. Types of Content Aware Policies 64
7.2.4. Setting up Content Aware Policies 65
7.3. Custom Content Dictionaries 70
7.4. Content Aware URL Whitelists 71
7.5. Content Aware Domain Whitelists 71
7.6. Content Aware Regex (Regular Expressions) 72
7.7. How Content Aware Protection works for monitored Applications / Online Services 74
8. Reports and Analysis 75
8.1. Logs Report 76
8.2. File Tracing 77
8.3. File Shadowing 78
8.4. Content Aware Report 79
8.5. Content Aware File Shadowing 80
8.6. Admin Actions 81
8.7. Online Computers 82
8.8. Online Users 82
8.9. Online Devices 84
8.10. Computer History 85
8.11. User History 86
8.12. Device History 87
8.13. Statistics 88
9. Alerts 89
9.1. Define System Alerts 91

9.2. Define Alerts (Device Control Alerts) 93
9.3. Define Content Aware Alerts 95
9.4. Define MDM Alerts 96
9.5. System Alerts History 97
9.6. Alerts History 98
9.7. Content Aware Alerts History 99
9.8. MDM Alerts History 100
10. Directory Services 101
10.1. Active Directory Import 101
10.2. Active Directory Sync 104
11. System Maintenance 109
11.1. File Maintenance 109
11.2. System Snapshots 110
11.3. Log Backup 112
11.3.1. Backup Scheduler (Automatic Log Backup) 113
11.4. Content Aware Log Backup 115
11.4.1. Automatic Scheduler (Automatic CAP Log Backup) 116
12. System Configuration 118
12.1. Client Software 118
12.2. Client Software Upgrade 119
12.3. Client Uninstall 120
12.4. EasyLock Software Download 121
12.5. System Administrators 122
12.6. System Departments 123
12.7. System Security / Client Uninstall Protection 125
12.8. System Policies 126
12.9. System Settings 128
12.10. System Licensing 129
12.10.1. Appetizer Mode 131
12.10.2. Trial Mode 132
12.10.3. Import Licenses 132

13. System Parameters 135
13.1. Device Types 135
13.2. Rights 136
13.3. Events 137
13.4. File Types 138
14. Setting up Policies 139
15. Modes for Users, Computers and Groups141
15.1. Transparent Mode 142
15.2. Stealth Mode 142
15.3. Panic Mode 142
15.4. Hidden Icon Mode 143
15.5. Silent Mode 143
15.6. Adding new administrator(s) 144
15.7. Working with logs and reports 146
16. Enforced Encryption with Trusted Devices 147
16.1. How a Level 1 Trusted Device Works 148
16.2. EasyLock Software for Trusted Devices Level 1 149
16.2.1. Managing Trusted Devices from EPP server console 149
16.2.2. File Tracing on EasyLock 2 TrustedDevices 150
17. Endpoint Protector Client 152
17.1. Endpoint Protector Client Installation 152
17.2. Endpoint Protector Client Security 153
17.3. Client Notifications (Notifier) 154
17.4. Client Policy Update 154
17.5. Offline Functionality for Endpoint Protector Client 154
17.6. DHCP / Manual IP address 155
17.7. Client Removal 155
17.7.1. Client Removal on Windows OS 155
17.7.2. Client removal on MAC OS X.....155

17.7.3. Client removal on Linux OS 155
18. Installing Root Certificates to your Internet Browser 156
18.1. For Microsoft Internet Explorer 156
18.2. For Mozilla Firefox 165
19. Terms and Definitions 167
19.1. Server Related 167
19.2. Client Related 168
20. Support 170
21. Important Notice / Disclaimer 171

1. Introduction

Portable storage devices such as USB flash drives, external HDDs, digital cameras and MP3 players/iPods are virtually everywhere and are connected to a Windows PC, Macintosh or Linux computer via plug and play within seconds.

With virtually every PC, MAC or Linux workstation having easily accessible USB, FireWire and other ports, the theft of data or accidental loss of data is for individuals a mere child's play.

Data theft or data loss or infecting companies' computers or network through a simple connection is easy and doesn't take more than a minute. Network administrators have little chance to prevent this from happening or to catch the responsible user(s). Now Endpoint Protector, through its Device Control module, helps companies to stop these threats.

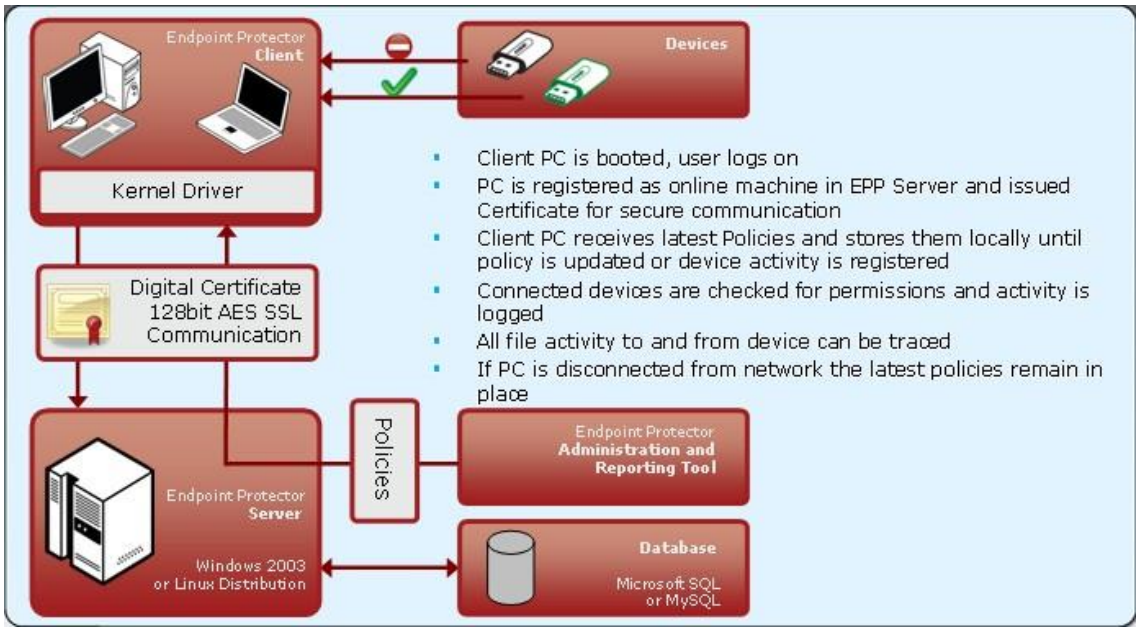
As a complete Data Loss Prevention solution, Endpoint Protector not only controls all device activity at endpoints, but monitors and scans all possible exit points for sensitive content detection. Its second module, Content Aware Protection, ensures that no critical business data leaves the internal network either by being copied on devices or sent via the Internet without authorization, reporting all sensitive data incidents.

1.1. What is Endpoint Protector?

Endpoint Protector will help you secure your PCs endpoints within your network and screen all possible exit ways for sensitive content detection. You will be able to restrict the use of both internal and external devices which can be used for data storage and transfer and to manage PC, MAC and Linux ports.

Endpoint Protector, through its two main modules, Device Control and Content Aware Protection gives network administrators the control needed to keep network endpoints safe:

- Control use of all USB and other storage devices
- Tracking of what data is saved to storage devices
- Tracking of what data is copied from and to storage devices
- Scanning of all data transfers for sensitive content detection
- Complete monitoring of all possible data exit points
- Authorize the use of USB storage devices
- Securing data on USB storage devices
- Powerful reporting tool and audit


Endpoint Protector
Client
Kernel Driver
Devices
Digital Certificate
128bit AES SSL
Communication
Client PC is booted, user logs on
PC is registered as online machine in EPP Server and issued Certificate for secure communication
Client PC receives latest Policies and stores them locally until policy is updated or device activity is registered
Connected devices are checked for permissions and activity is logged
All file activity to and from device can be traced
If PC is disconnected from network the latest policies remain in place
Policies
Endpoint Protector
Server
Windows 2003
or Linux Distribution
Endpoint Protector
Administration and
Reporting Tool
Database
Microsoft SQL
or MySQL

The modular and intuitive Web-based administration interface has been designed to offer fast access to controlling computer, devices and user behavior in a large network. It also offers several ways to track any kind of portable device related activity registered on the system. A detailed report including timestamps, file

names, action(s) taken, logged user, etc. allows for pin-pointing malicious behavior and users.

The system's design also allows the CoSoSys team to perform easy customizations and extensions requested by clients. Better automation and express reports can be developed accordingly to customer demands. In the same time this structure is easy to update and maintain, making the usability even greater.

Endpoint Protector is the only solution that gives companies of any size the ability to let users take advantage of the increasingly important functionality of USB and other ports without losing control over data and compliance.

This endpoint security device control solution is designed to control usage of all portable storage and to keep track of what data users are taking from and to their work computers on any kind of portable storage devices.

Furthermore, Endpoint Protector enables network administrators to monitor and report what data is introduced into the corporate network from a portable storage device such as prohibited materials (MP3s, movies or games) or harmful data like a virus that could jeopardize the networks integrity.

As not all portable storage devices are used with the intent to harm the company, many legitimate reasons commonly justify the need of such devices to increase network users' productivity. Thus, Endpoint Protector allows authorized use of certain device types or specific devices such as the companies' own USB Flash Drives to handle and transfer confidential data.

To ensure the protection of data carried by users on authorized devices, the Endpoint Protector administrator can allows users to copy work data only to a password protected / encrypted area of an authorized device, a so called "Trusted Device". In this way confidential corporate data is protected in case of hardware loss.

Endpoint Protector creates an audit trail that shows the use and activity of portable storage devices in corporate networks. Thus, administrators have the possibility to trace and track file transfers through endpoints and then use the audit trail as legal evidence for data theft. For more details on Endpoint Protector, please see the Data Sheet available on the company's website.

http://www.EndpointProtector.com

1.2. Main Features

Your confidential sensitive data is only as safe as your endpoints are. Designed for medium and large enterprises, Endpoint Protector offers powerful features in order to control monitor and enforce network and endpoint security.

Endpoint Security for Windows, Macintosh and Linux Workstations, Notebooks and Netbooks.

Endpoint Protectors full feature set is available for Windows. A reduced feature set is available for Macintosh (OS X) and Linux - Ubuntu 10.04 LTS and openSUSE 11.4.

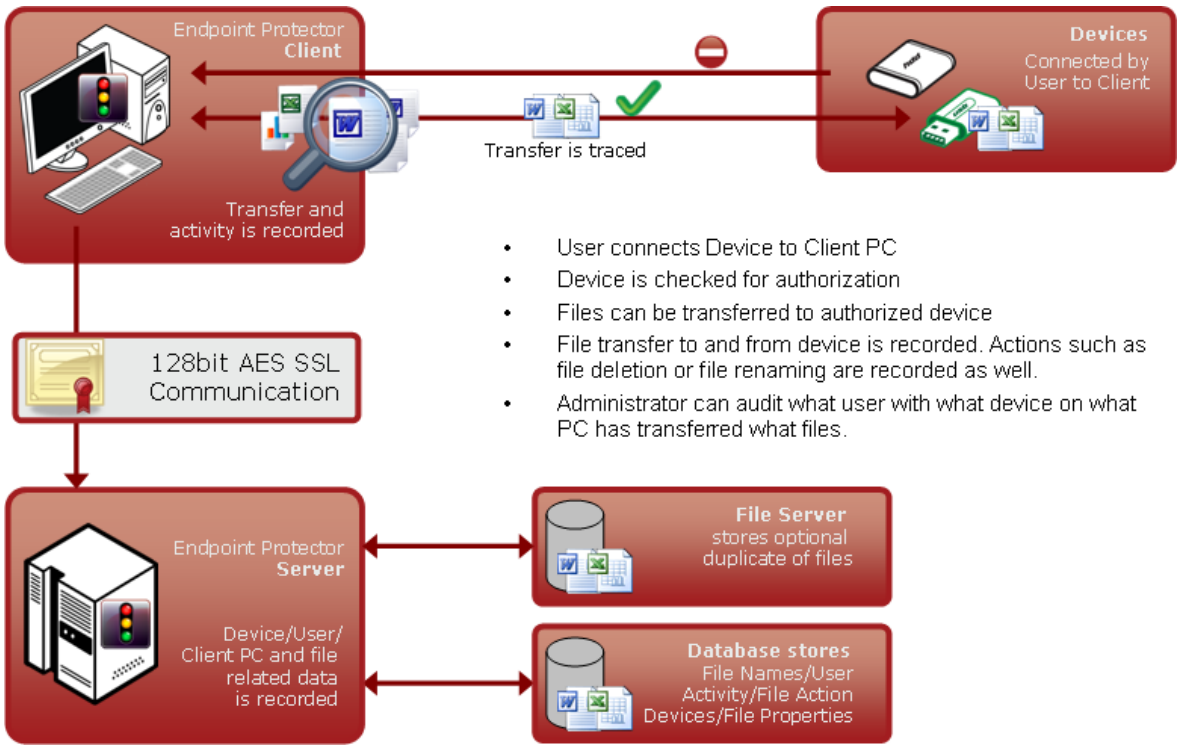
Protects PCs from threats posed by removable portable storage and endpoint devices like USB Flash Drives, MP3 Players, iPods, digital cameras and other devices that could be intentionally or accidentally used to leak, steal, lose, virus or malware infect your data. Even self-executing devices like a USB Flash Drive with a CD-ROM autorun feature such as U3 Drives will not be accessible and thereby pose no threats.

1.2.1. Centralized web based Device Management / Dashboard

Network administrators have the ability to centrally manage and authorize the use of devices. The Endpoint Protector 4 Dashboard is designed to meet the needs of both management and security staff and offer access to real-time information, charts and reports about organization wide controlled device and data transfer activity. All in an integrated single view and Web based Administration and Reporting Tool.

1.2.2. Control your data flow: File Tracing / File Shadowing

This thorough record of information streams at the network’s endpoints is supporting audits of data flow and controlling the impact of data leakage. The File Tracing feature will track all data that was copied to and from prior authorized portable storage devices. The File Shadowing feature saves a copy of all, even deleted files that were used in connection with controlled devices on a network storage server.



1.2.3. Audit Trail – Device Activity Logging

A device activity log is recorded for all clients and devices connected along with all administrative actions such as device authorizations, giving a history for devices, PCs and users for future audits and detailed analysis.

1.2.4. Audit Trail – Reporting and Analysis Tools

Endpoint Protector 4 is equipped with powerful reporting and analysis tools to make the data audit process easy and straightforward.

1.2.5. Sensitive Content Filtering

Scans and reports all transfers of sensitive data on and from any removable media or via the Internet.

1.2.6. File Whitelist

Allows only previously authorized files to be copied to portable storage devices.

1.2.7. Easy Enforcement of Your Security Policies

Simplified device management policies with customizable templates for defining User Group permissions allow easy enforcement and maintenance of your latest security policies across your network.

1.2.8. Network "Offline" Mode to Support Your Field Employees

"Offline Temporary Password" to allow time limited access to a specific device when the client computer is disconnected from the network.

Protected PCs that are temporary or frequently disconnected from the network like laptops stay protected based on the last locally saved policy. All notifications are transmitted at the next network connection.

1.2.9. Enforced Encryption - protecting sensitive data in transit / Trusted Device

The technology behind Trusted Devices is designed to certify that in the corporate environment all the endpoint devices are not only authorized and controlled via endpoint software and security policies but also certified and trusted for protecting sensitive and confidential data in transit (in case of a Trusted Device). This will assure that in the event a device is stolen or lost all the data stored on it is encrypted and therefore not accessible for other parties.

1.2.10. Client Uninstall Protection

Endpoint Protector 4 offers a password-based solution that prevents the users from uninstalling the Endpoint Protector Clients, thus ensuring continuous data protection.

1.2.11. Client Stop Protection / Tamper Protection

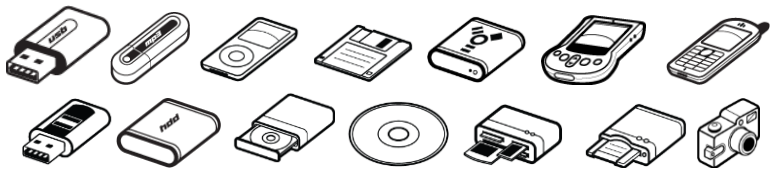
Endpoint Protector 4 prevents users from stopping the Endpoint Protector Clients at any time.

1.2.12. Backup Scheduler

Endpoint Protector 4 provides an automatic log backup solution in order to prevent the server from overloading.

1.3. Controlled Device Types / Ports

Endpoint Protector supports a wide range of device types which represent key sources of security breaches. These devices can be authorized which makes it possible for the users to view, create or modify their content and for administrators to view the data transferred to and from the authorized devices.



- Removable Storage Devices
- Normal USB Flash Drives, U3 and Autorun Drives, Disk on Key, etc.
- USB 1.1, USB 2.0, USB 3.0
- Wireless USB
- LPT/Parallel ports
  By controlling the Parallel ports of a PC using Endpoint Protector, the network administrator can deny or allow users access to storage devices connected to these ports.
  * APPLIES ONLY TO STORAGE DEVICES
- Floppy disk drives
  Access to floppy disk drives can be managed through Endpoint Protector and can be turned on/off completely.
- Memory Cards - SD Cards, MMC Cards, and Compact Flash Cards, etc.
  These devices can be enabled / disabled via Endpoint Protector.
- Card Readers - internal and external
  These devices can be enabled / disabled via Endpoint Protector.
- CD/DVD-Player/Burner - internal and external
  These devices can be enabled / disabled via Endpoint Protector.
- Digital Cameras
  These devices can be enabled / disabled via Endpoint Protector.

- Smartphones / Handhelds / PDAs
  This category includes Nokia N-Series, Blackberry, and Windows CE compatible devices, Windows Mobile devices, etc.

- iPods / iPhones / iPads
  These devices can be enabled / disabled via Endpoint Protector.

- MP3 Player / Media Player Devices
  These devices can be enabled / disabled via Endpoint Protector.

- External HDDs / portable hard disks
  These devices can be enabled / disabled via Endpoint Protector.

- FireWire Devices
  These devices can be enabled / disabled via Endpoint Protector.

- PCMCIA Devices
  These devices can be enabled / disabled via Endpoint Protector.

- Biometric Devices
  These devices can be enabled / disabled via Endpoint Protector.

- Bluetooth
  These devices can be enabled / disabled via Endpoint Protector.

- Printers
  Applies to serial, USB and LPT connection methods. These devices can be enabled / disabled via Endpoint Protector.

- ExpressCard (SSD)
  These devices can be enabled / disabled via Endpoint Protector.

1.4. Conclusions

As information theft and data leakage are a reality of today's business world, effectively preventing all possible security breaches is becoming an ultimate concern for enterprise security experts. Endpoint security comes to complete your existing security policies, aiming to render it full proof.

As new circumvention and data compromising techniques come to diminish the benefits of new devices and gadgets, Endpoint Protector secures your company's technologically enabled mobility. Thus, by easily protecting all exposed endpoints from inbound and outbound threats, you can enjoy enhanced portability, efficiency and productivity.

As it enables your employees to use devices you have already invested in and it protects your company from losses generated by attacks from outside and within, all financial costs entailed by implementing Endpoint Protector, such as purchase, implementation and usage training expenses, are fully justified by the yielded return on investment.

2. Server Functionality / Server Components

The functionality is designed to be around several physical entities:

- Computers (PCs, MACs and Linux workstations with Endpoint Protector Client installed)
- Devices (the devices which are currently supported by Endpoint Protector. e.g.: USB devices, digital photo cameras, USB memory cards etc)
- Client user (the user who will use the devices and the computers)

The server side of Endpoint Protector has different parts working close together:

- Web Service – responsible of communicating with the clients and storing the information received from them
- The Administration and Reporting Tool – responsible for managing the existing devices, computers, users, groups and their behavior in the entire system
- Endpoint Protector Appliance Hardware (Only applies if you have purchased the Endpoint Protector Hardware Appliance) – is the hardware running the Endpoint Protector Server containing Operating System, Database, etc.

2.1. Endpoint Protector – Web Service

The Web Service of Endpoint Protector is responsible for the communication between Endpoint Protector Server and the Client computers. Starting with the registration of the client computers, the Web Service sends the settings and rights of each computer and also receives the log information from each client and stores that information in the database.

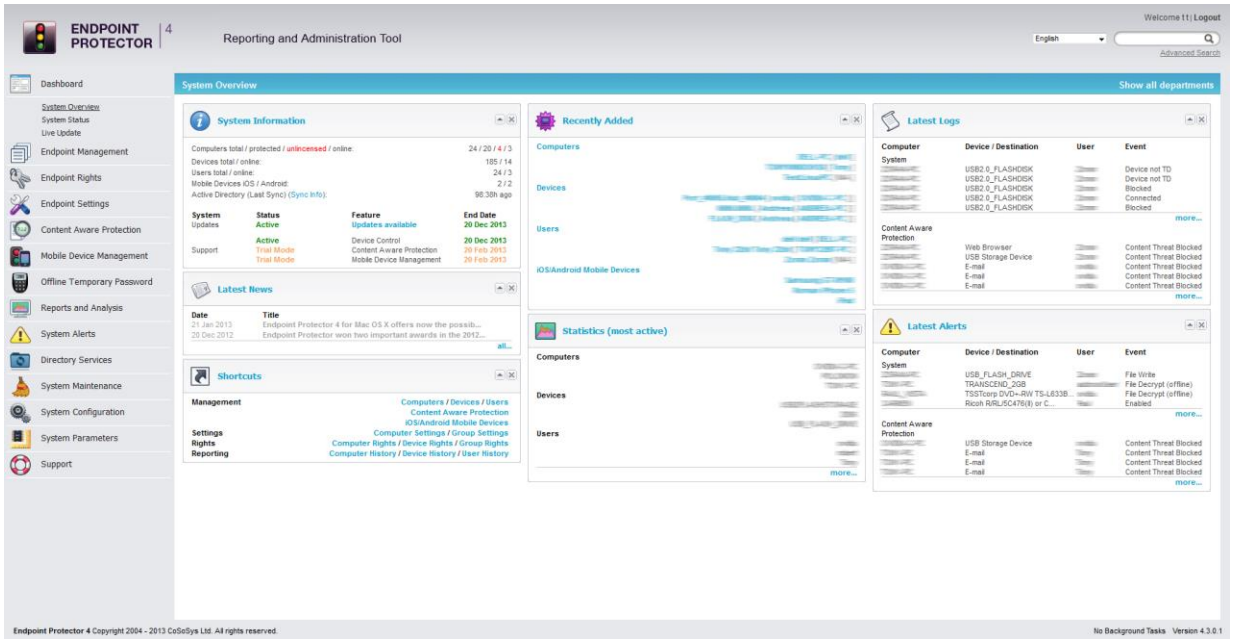
The Web Service is started as long as the Web server is running, and it is ready to respond to each client request.

2.2. Administration and Reporting Tool

This part of the Server is designated as a tool for customizing the behavior of the entire system (Server and Clients) and to offer the administrator(s) (the person handling this tool) the necessary information regarding the activity on the system.

Access to this part of the Web server is restricted by a username/password pair. The users accessing the Web application are referred to as Administrator in this document. This administrator can be a regular administrator or super administrator. The difference between the two is the level of access to some administrative parts of the application. The regular administrator cannot change critical system parameters, cannot create/delete other administrators and has restricted access to some areas of Endpoint Protector.

Dashboard – Lets you view statistics of the server such as the number of clients and devices currently connected, total number of computers, log and shadow size, last logged action, newest added client, latest news about the product and the company, licensing status, etc. and also provides shortcuts to the essential management tools.



Endpoint Management – Used for administration of Devices, Computers, Groups, and Client Users.

In this module, the administrator can edit, manage rights and settings for or even delete devices, computers or groups. He can also create groups and add or remove client users.

Endpoint Rights – Used to determine and define rules of access. Six subsections are found here Devices Rights, User Rights, Computers Rights, Group Rights, Global Rights, Effective Rights and File Whitelist.

This is the most important module of Endpoint Protector. In this module the administrator can set up and enforce security policies by assigning specific rights to devices, computers, computer groups and global device access. Please refer to section 4 "Endpoint Rights" for more information.

Endpoint Settings – Used for setting the behavior of computers, groups of computers or all the computers.

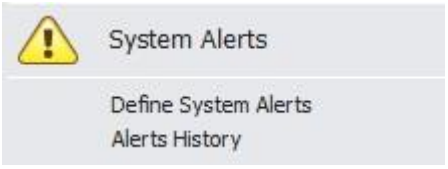
In this module the administrator can modify global settings such as the log upload interval, local log and shadow size, as well as manage computer and computer group's settings. The functionality mode (Normal, Stealth, Transparent, etc) can also be set from here.

Content Aware Protection – Separate module, which allows creating and enforcing strong content aware policies for a better control of what data leaves the company network via any removable media or the Internet.

Reports and Analysis – Designed to offer the administrator information regarding the past and current activity on the system (Server and Clients). It includes several sections such as Online Computers, Online Users, Statistics, Graphics, etc. Several information formats are available for view and export.

Similar to the Dashboard, this module displays usage statistics on past and current activities, but with more details.

System Alerts – Allows the creation of System Alerts – notifications, set up by administrators, which will alert them if a certain device was connected or accessed, a certain user performed a certain action, etc. Please see paragraph 8 "Alerts" for more details.



System Parameters – Here you can determine the functionality of the entire system. This module includes sections such as Device and File Types, Rights and Events.

2.3. Accessing the Administration and Reporting Tool

To access the Administration and Reporting Tool, simply open a browser and enter the IP address of the Endpoint Protector Server, the Endpoint Protector Appliance IP or the Server Host Name.

In case you enter the IP address, please note that you must use the HTTPS (Hypertext Transfer Protocol Secure) prefix, followed by the IP address of the Endpoint Protector Server.

Example: https://127.0.0.1/index.php.

(In case of using the Endpoint Protector Appliance the default IP address is https://192.168.0.201).

If you use Internet Explorer, we recommend that you add this page to Internet Explorer's trusted sites. To do this, follow the steps in paragraph 18 "Installing Root Certificates to your Internet Browser".

2.4. Login Credentials (Username and Password)

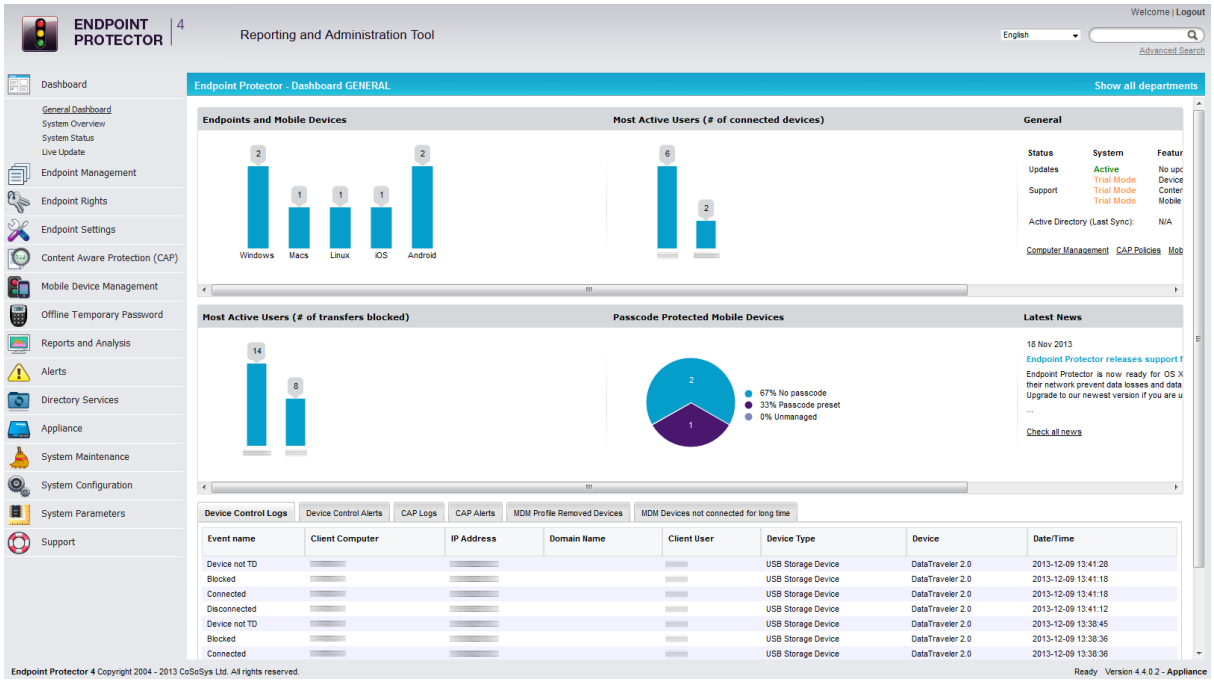
The default username and password for Endpoint Protector 4 Administration and Reporting Tool are:

USERNAME: root
PASSWORD: epp2011

To change the username and password and to create additional administrators, please see paragraph 11.2 "System Administrators".

2.5. General Dashboard

Some of the most important activities logged by EPP can be monitored under this tab. The image below is self-explanatory.



More specific dashboards are available at Endpoint Management, Content Aware Protection and Mobile Device Management.

2.6. System Status

Under the System Status tab from the Dashboard module, you can access the "System Lockdown", "Endpoint Protector ON/OFF" , "Content Aware Protection ON/OFF", "Custom Classes ON/OFF" buttons.

System Lockdown - Pressing this button will cause Endpoint Protector to instantly deny access to all devices in the system, stopping also ongoing data transfers (depending on device type). Log files are still created of what was accessed or modified before the Lockdown button was pushed.

Endpoint Protector ON/OFF – Pressing this button (OFF) will stop all Endpoint Protector related activities completely. This means that all devices, even those previously blocked, will now be usable, logging of traffic will stop as well as file shadowing.

Content Aware Protection ON/OFF – Pressing this button (OFF) will stop all Content Aware Protection related activities completely. This means that all files that are sensitive or are containing sensitive data will not be detected and will not be reported.

Custom Classes ON/OFF – Pressing this button (ON) will enable custom classes. The administrator can create in the Endpoint Management / Custom Classes tab separate rights for devices that will override all rights set for those devices in the Endpoint Rights tab.

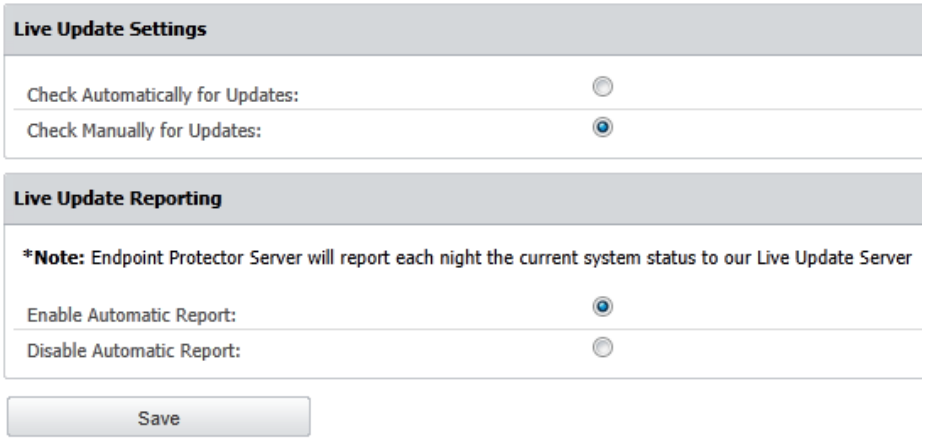
The "**Re-read**" command will force all computers to re-read their rights at the next refresh interval.

2.7. Live Update

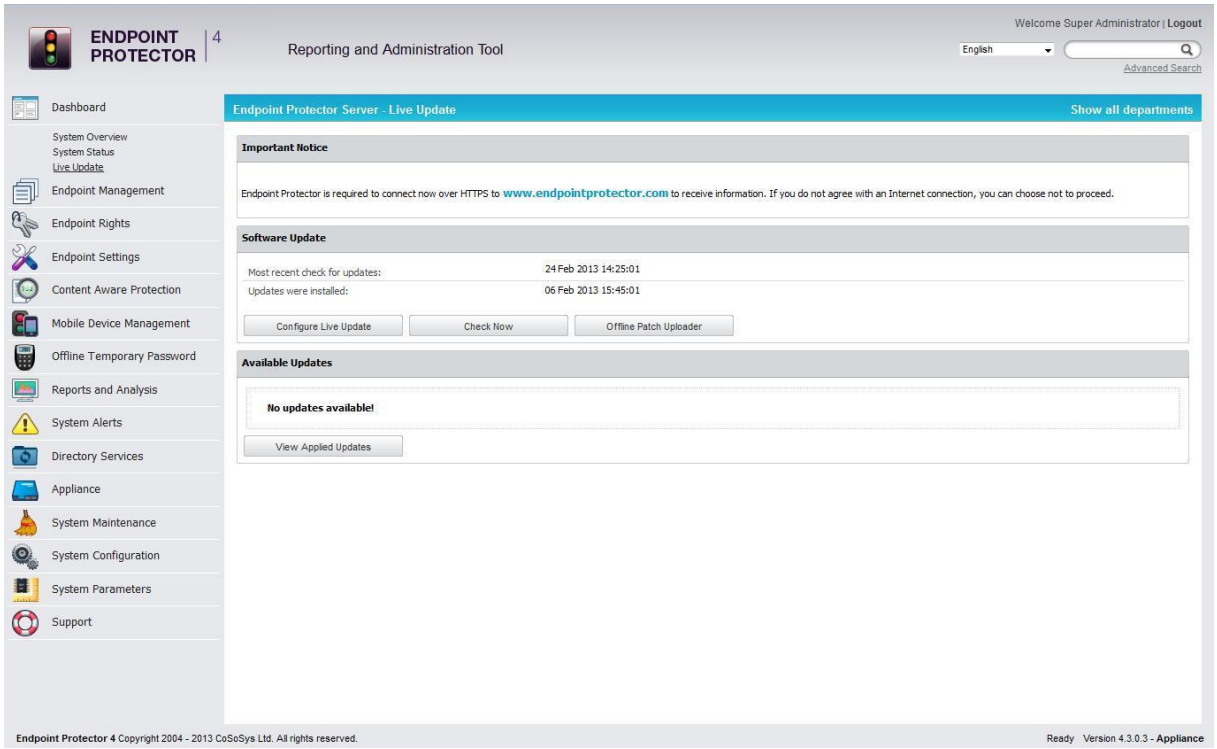
This section allows checking and applying the latest Endpoint Protector Server updates. Please note that this feature communicates through port 80.

The two options available are:

- Configure Live Update – allows selecting one of the two options for performing the live update check: manually or automatically and enabling or disabling the Automatic Reporting to the Live Update Server


Live Update Settings
Check Automatically for Updates:
Check Manually for Updates:
Live Update Reporting
*Note: Endpoint Protector Server will report each night the current system status to our Live Update Server
Enable Automatic Report:
Disable Automatic Report:
Save

- Check Now – searches for the latest Endpoint Protector Server updates.



In case that new updates are found, they are displayed under the Available Updates window section and can be directly installed by pressing on the "Apply Updates" button. The latest installed updates can be checked by pressing on the "View Applied Updates" button.

- Offline Patch Uploader - offers the possibility to upload updates in offline mode, without an internet connection

Note!

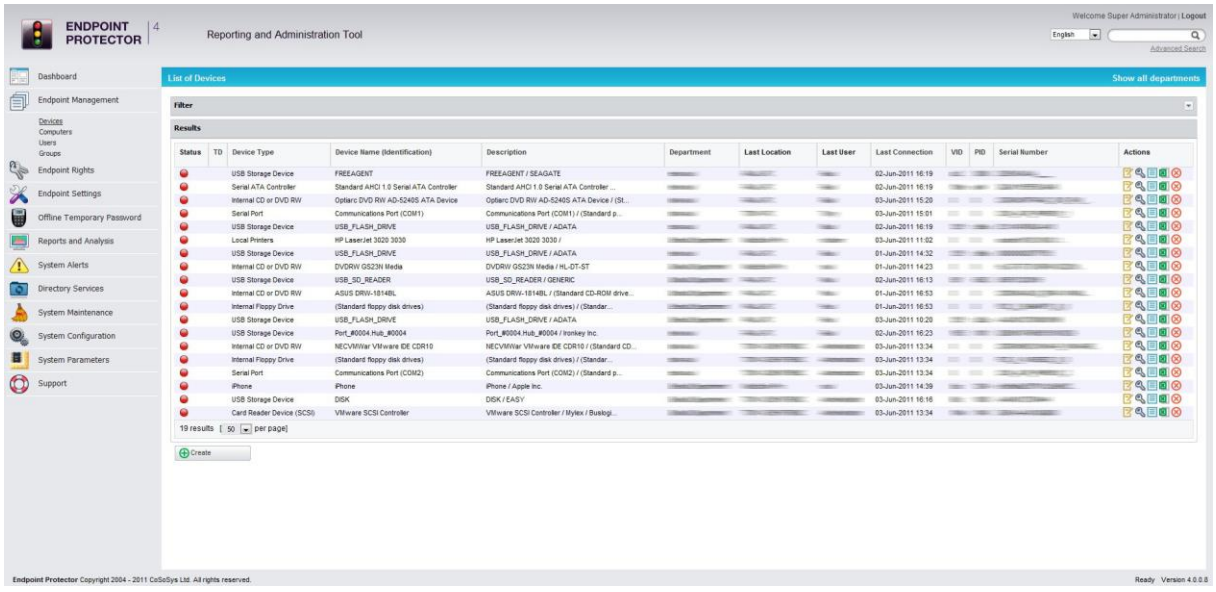
Contact support@endpointprotector.com to request the Offline Patch.

3. Endpoint Management

3.1. Devices

In this module the administrator can manage all devices in the system. Endpoint Protector has an automatic system implemented meaning that it will automatically add any unknown devices connected to client computers to the database, thus making them manageable.

When an unknown device is connected to one of the client computers, the device's parameters are stored in the system database as: device data (Vendor ID, Product ID, and Serial Number). The user who first used the device is stored as the default user of the device. This, however, can be changed anytime, later.



These are the actions available to the administrator in this module:

Edit, Manage Rights, Device History, Export Device History, Delete

Manage Rights and Device History are actually shortcuts to the Devices Rights and Logs Report modules, and will be explained in one of the following chapters.

The status column indicates the current rights for the devices.

Red means that the device is blocked in the system.

Green means that the device is allowed on computers or users.

Yellow means that device is allowed on some users or computers with restrictions.

3.2. Device Functionality

Endpoint Protector can handle a wide variety of devices and device types and offers several methods of usage for each device in particular. These can be found by accessing the "Endpoint Rights" module of Endpoint Protector and selecting one of the relevant Rights tabs. The Endpoint Rights module contains the following sections: Device Rights, User Rights, Computer Rights, Group Rights, Global Rights, Effective Rights and File Whitelist.

Depending on the network policy, administrators can use the following settings:

- Preserve Global settings
- Deny access to devices
- Allow access to devices
- Enable read-only access
- Trusted Device Level 1 to Level 4

Allow Access
Preserve global setting
Deny Access
Allow Access
Read Only Access
Allow Access if TD Level 1
Allow Access if TD Level 2
Allow Access if TD Level 3
Allow Access if TD Level 4

3.2.1. Give / Deny Access to Devices

With this option the administrator can give or deny complete access to a certain device making it usable or obsolete for a certain group, computer or user.

The administrator can configure these settings for each device individually and can also choose for what computer(s), user(s) and group(s) they will apply to.

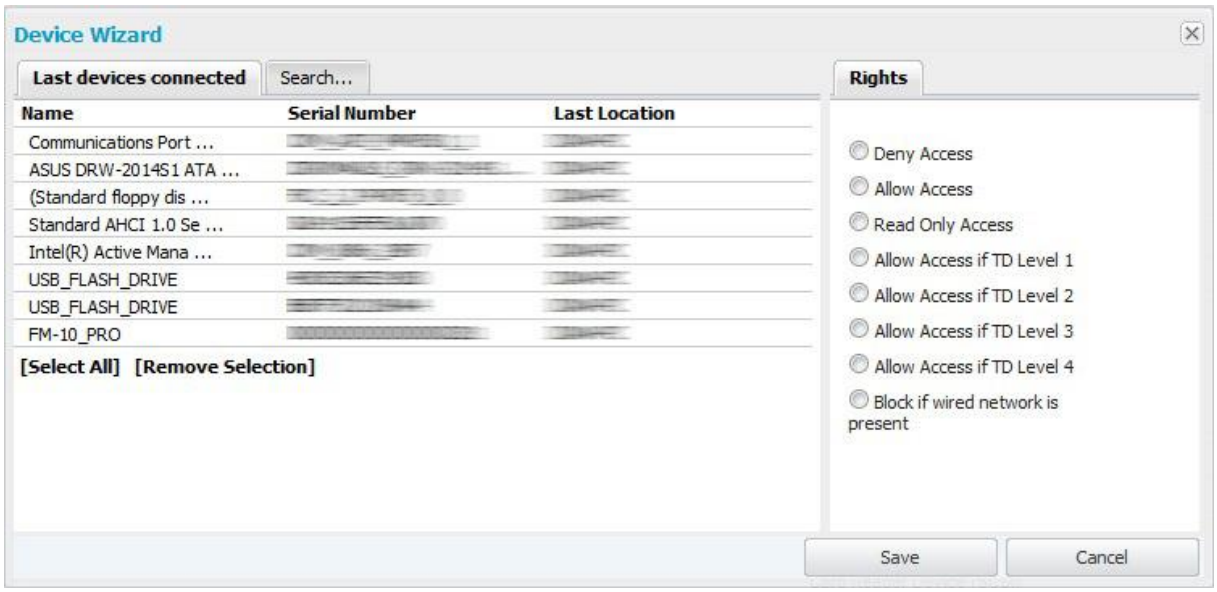
The File Whitelisting feature allows the super administrator to control the transfer of only authorized files to previously authorized portable storage devices.

To configure File Whitelisting, please see paragraph 4.7 "File Whitelist".

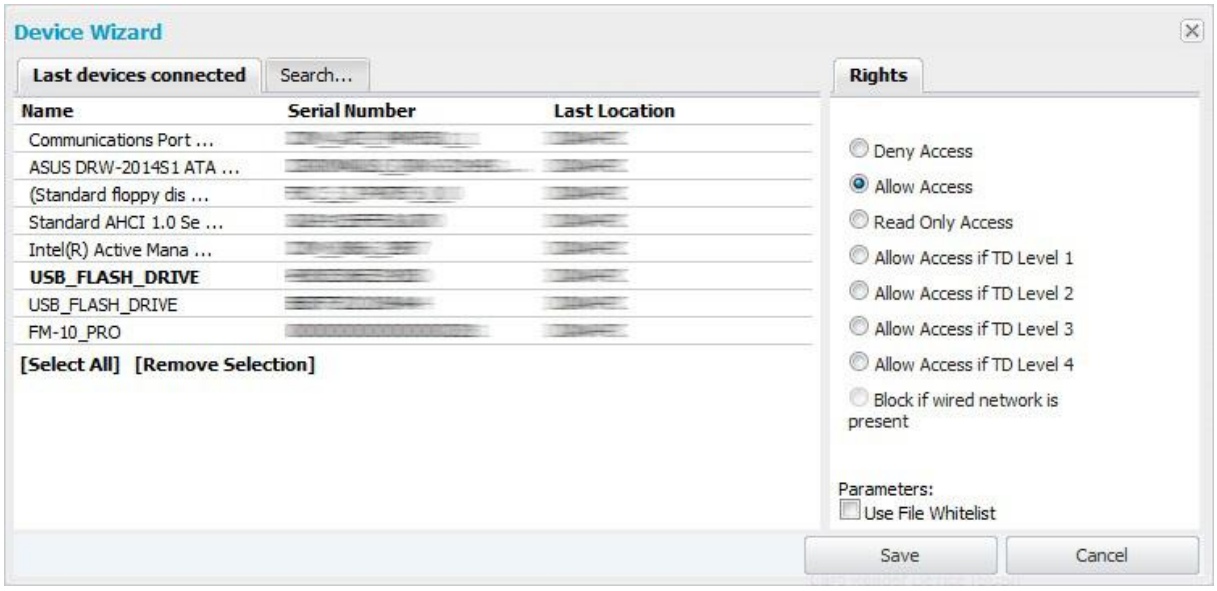
Once configured, you can enable this feature for devices, users, computers and groups. To do this, simply access the Endpoint Rights module and select device, computer, user or group rights, depending on the rights priority configuration of your server.

Select the device, user, computer or group you wish to manage rights for and click the + (plus) button at the bottom of the page, under "Already Existing Devices"

Once you do that, the Device Wizard will appear, allowing you to select the device(s) you wish to manage. Please note that you need to allow access to the storage device in order to enable the File Whitelisting for it.



Selecting a device will allow you to select one of the rights for that device.



Once you select a portable device, and choose "Allow Access" for it, you will also have the option to enable File Whitelisting for that device.

Click "Save" to store your changes.

The device(s) you selected will appear in the "Already Existing Devices" section.

To add more devices, simply repeat the steps mentioned above.

To change or delete added devices use either “Rights Wizard” or “Remove” action buttons.

3.2.2. Enable Device Read-Only Access

With this option the administrator can enable read-only access to devices preventing the deletion or alteration of data on the device(s).

The administrator can configure each device individually and can also choose for what computer(s), user(s) and group(s) it will apply to.

3.2.3. TrustedDevice Level 1 to Level 4

The TrustedDevices™ technology integrated within Endpoint Protector is available in four security levels, depending on the degree of protection offered by a device (devices using EasyLock™ are TD level 1).

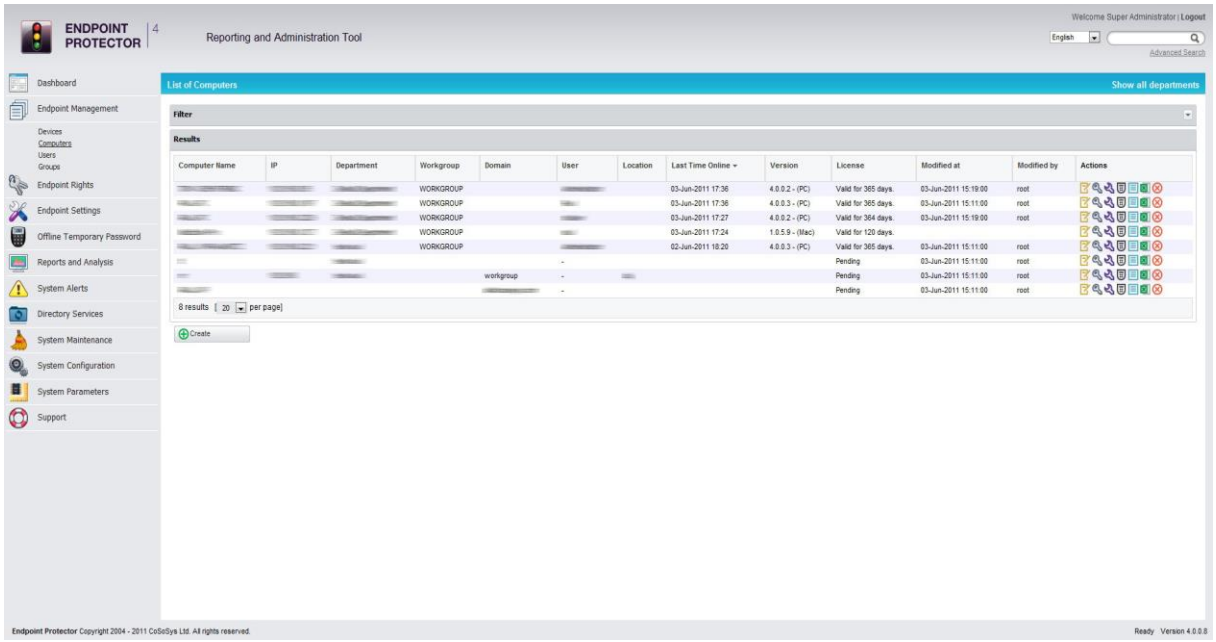
For more information on TrustedDevices™ and EasyLock™, refer to section 15. “Enforced Encryption with TrustedDevice” in this user manual.

3.2.4. WiFi - Block if wired network is present

With this option the administrator can disable the WiFi connection, while a wired network connection is present. The WiFi connection will be available when the wired network is not present.

3.3. Computers

This is the module responsible for managing the client computers.



The client computers have a registration mechanism. This self-registration mechanism is run once after the Endpoint Protector Client software is installed on a client computer. The client software will then communicate to the server its existence in the system. The server will store the information regarding the client computer in the system database and it will assign a license to the client computer (if none available, a demo license will be created and assigned, which will expire after 30 days).

NOTE!

The self-registration mechanism acts whenever a change in the computer licensing module is made, and also each time the application client is reinstalled. The owner of the computer is not saved in the process of self-registration.

Computers can also be imported into Endpoint Protector from Active Directory using the Active Directory Plug-in.

For details, please see paragraph 10.1 “Active Directory Import”.

The available actions here are:

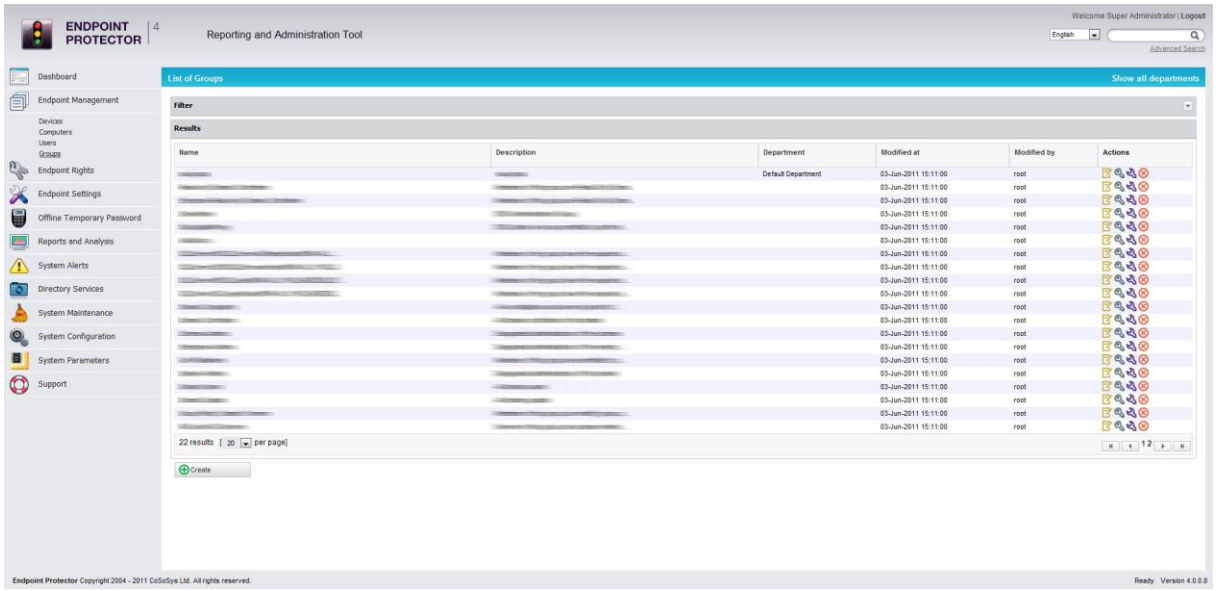
Edit, Manage Rights, Manage Settings, Offline Temporary Password, Computer History, Export Computer History and Delete. The Manage

Rights, Manage Settings, Offline Temporary Password and Computer History are links to their respective modules, which will be explained in their own chapter.

For a better organization and manageability, a computer can be assigned as belonging to a Group (several computers within the same office, a group of computers which will have same access rights or settings) or to a Department (an alternative organization to groups). For more details about departments, please see paragraph 11.3 “System Departments”.

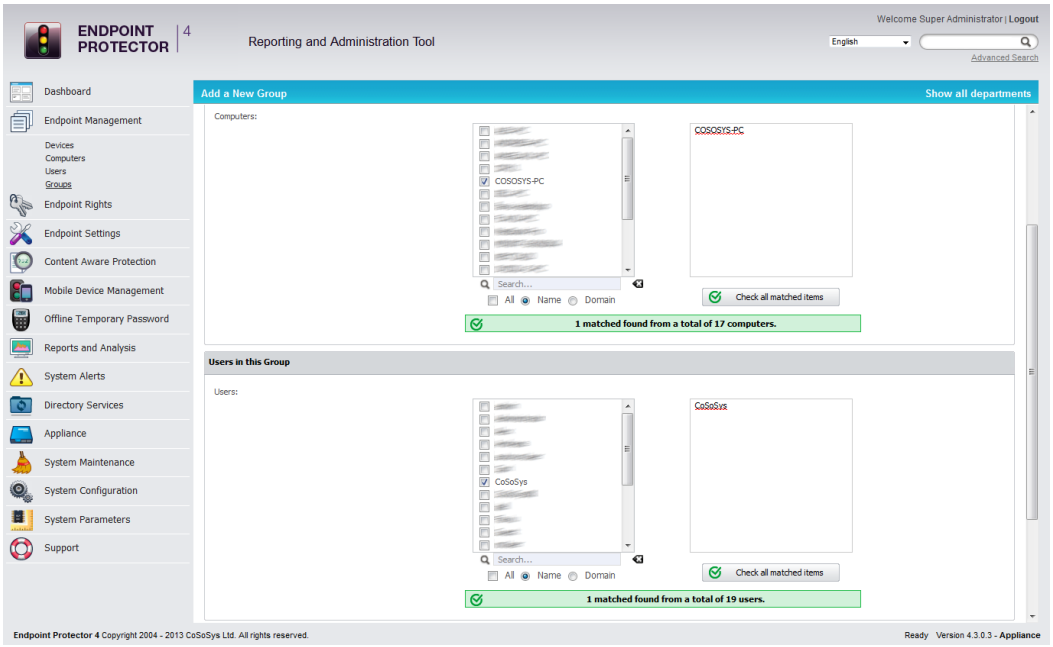
3.4. Groups

This module is responsible for editing groups. **Edit**, **Manage Rights**, **Manage Settings** and **Delete** are the commands available from this section.



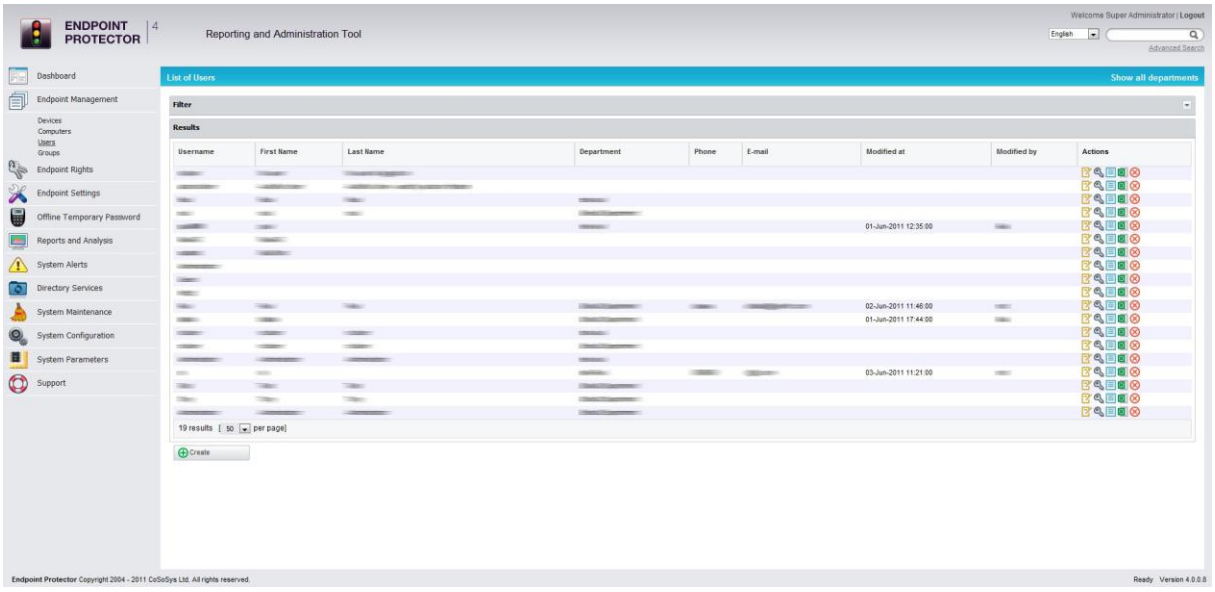
Grouping computers and client users will help the administrator to manage the rights, or settings for these entities in an efficient way. This can be done from the Group Rights and Group Settings tabs.

When creating a new group there is the possibility to add multiple users / computers simultaneously, by using the checkboxes and the option “Check all matched items”.



3.5. Users

The client users are the end users who are logged on a computer on which the Endpoint Protector Client software is installed.



This module has a self-completing mechanism: as soon as a user has some activity on the system and he is new in the system, he will be added to the system database.

Actions available in this group are: **Edit, Manage Rights, User History, Export User History** and **Delete**.

There are two users created by default during the installation process of Endpoint Protector.

noUser – is the user linked to all events performed while no user was logged in to the computer. Remote users' names who log into the computer will not be logged and their events will be stored as events of noUser. Another occurrence of noUser events would be to have an automated script/software which accesses a device when no user is logged in to the specific computer.

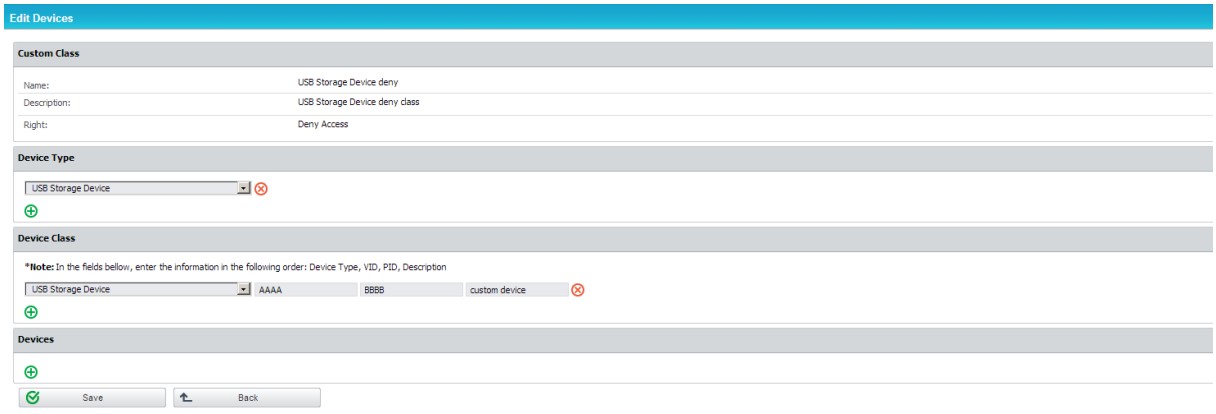
autorunUser – indicates that an installer has been launched by Windows from the specific device. It is the user attached to all events generated by the programs launched from the specific device when Autoplay is enabled in the Operating System.

The users can be arranged in groups for easier management at a later point. Users can also be imported into Endpoint Protector from Active Directory through the Active Directory Plug-in.

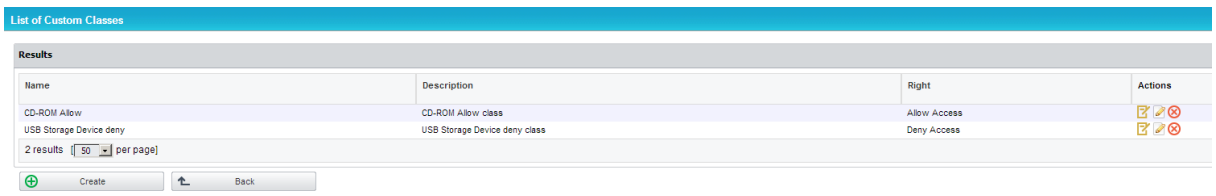
For details, please see paragraph 10.1 "Active Directory Import".

3.6. Custom Classes

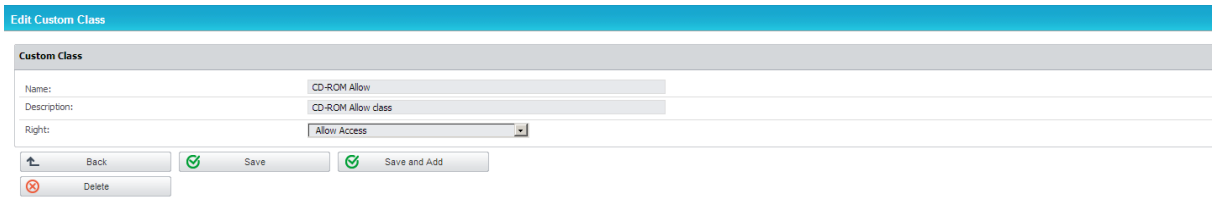
This module is responsible for creating new classes of devices for an easier management inside the system. It is a powerful function especially for devices belonging to the same vendor and/or being the same product (same VID and/or PID).



By selecting Endpoint Management > Custom Classes, the administrator is able to create and edit custom classes by adding new entities to the existing ones.



When creating a new custom class or editing an existing one, the administrator may provide a unique name and a short description, followed by the specification of the rights that will be automatically applied to all included devices.



Note!

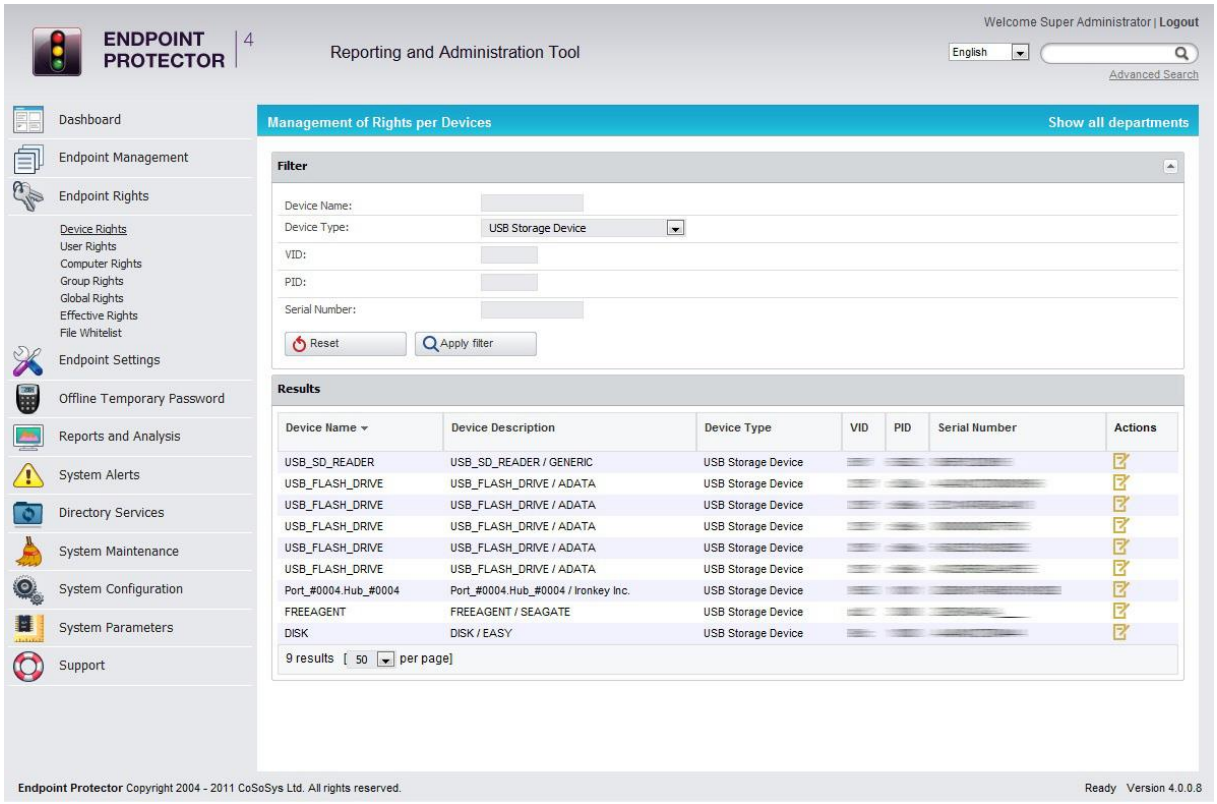
The rights set for a Custom Class will override all the other existing rights for the devices included in the newly created class and they will apply for any Endpoint Protector Client PC.

Example:

For the case above, we created a Custom Class *CD-ROM Allow* and set "Allow access" rights to devices of type CD-ROM /DVD-ROM. Let's say that CD-ROMs have "Deny access" rights set on Client PC CIP0. Once the custom class *CD-ROM Allow* is created and Custom Classes is enabled, all the CD-ROMs/DVD-ROMs will have access, even if on the Client PC CIP0 they have "Deny access".

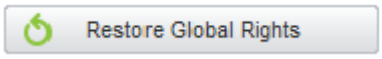
4. Endpoint Rights

The modules in this area will allow the administrator to define which device can be used on computers, groups and which client users have access to them.



The rule of inheritance is as follows (from most important to least important): Computer Rights -> Group Rights -> Global Rights. The rights are overwritten in this order.

Example: If global rights indicate that no computer on the system has access to a specific device, and for one computer that device has been authorized, then that computer will have access to that device.

"Restore Global Rights" () button can be used to revert to a lower level of rights. Once this button is pushed all rights on that level will be set to "preserve global settings" and the system will use the next level of rights.

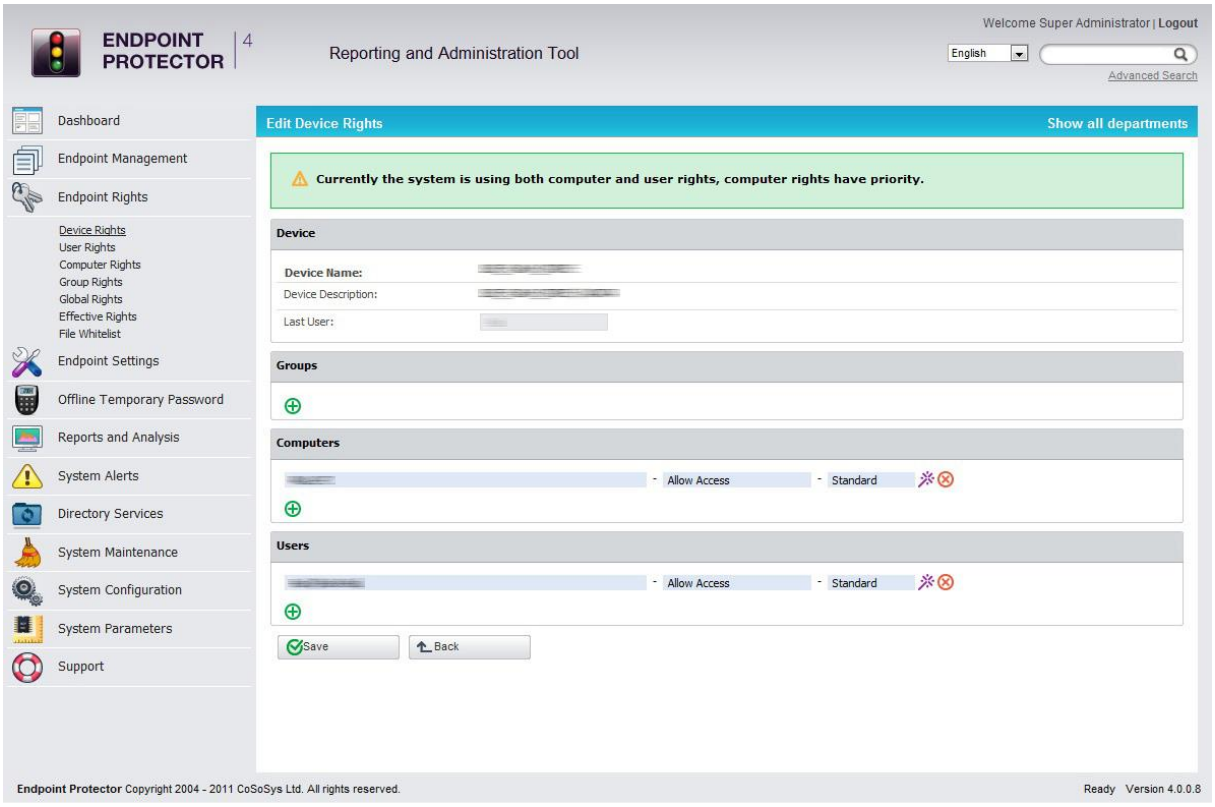
Example: If the action is done on group rights, the entities from that group will use from that point onwards the global rights.

Note!

All "already existing devices" that were added on that level will be deleted when the restore is used.

4.1. Device Rights

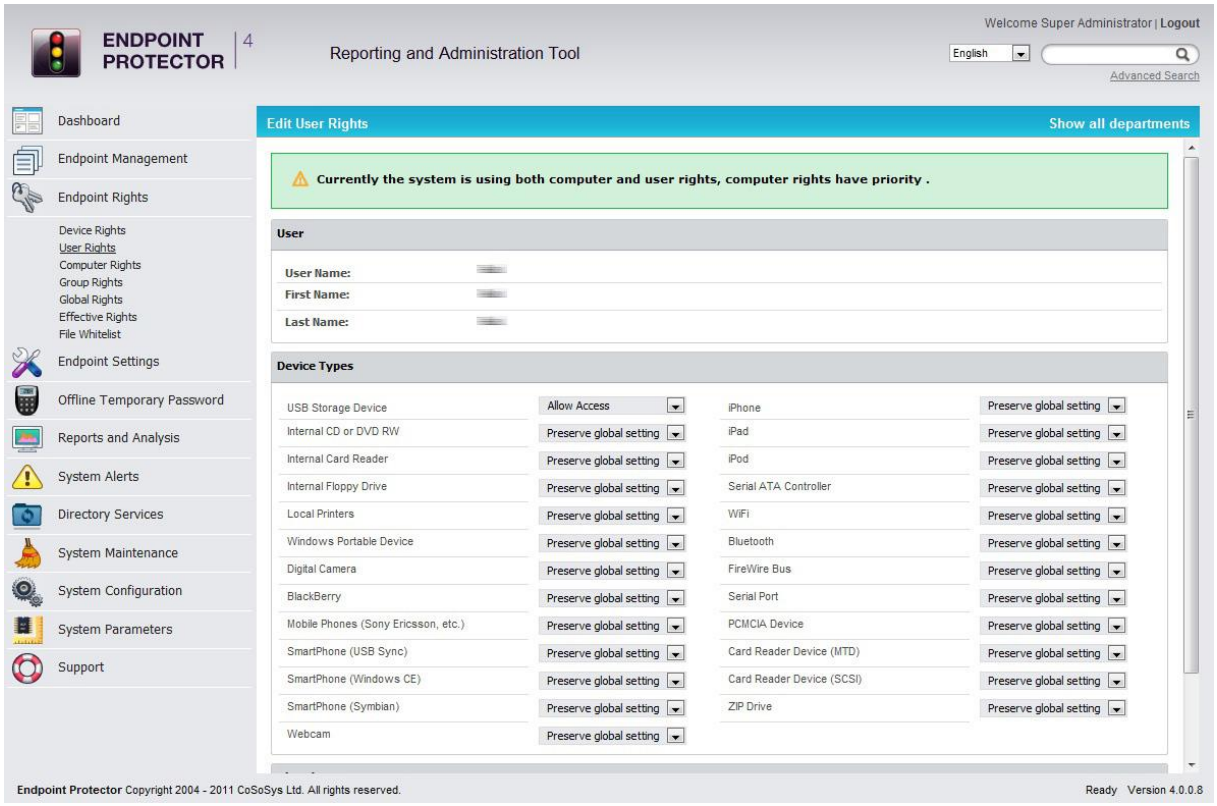
This module is built around the devices, allowing the administrator to enable or disable them for specific computers, groups or users.



After selecting a computer, you select the computers and group of computers for which the device has specified rights.

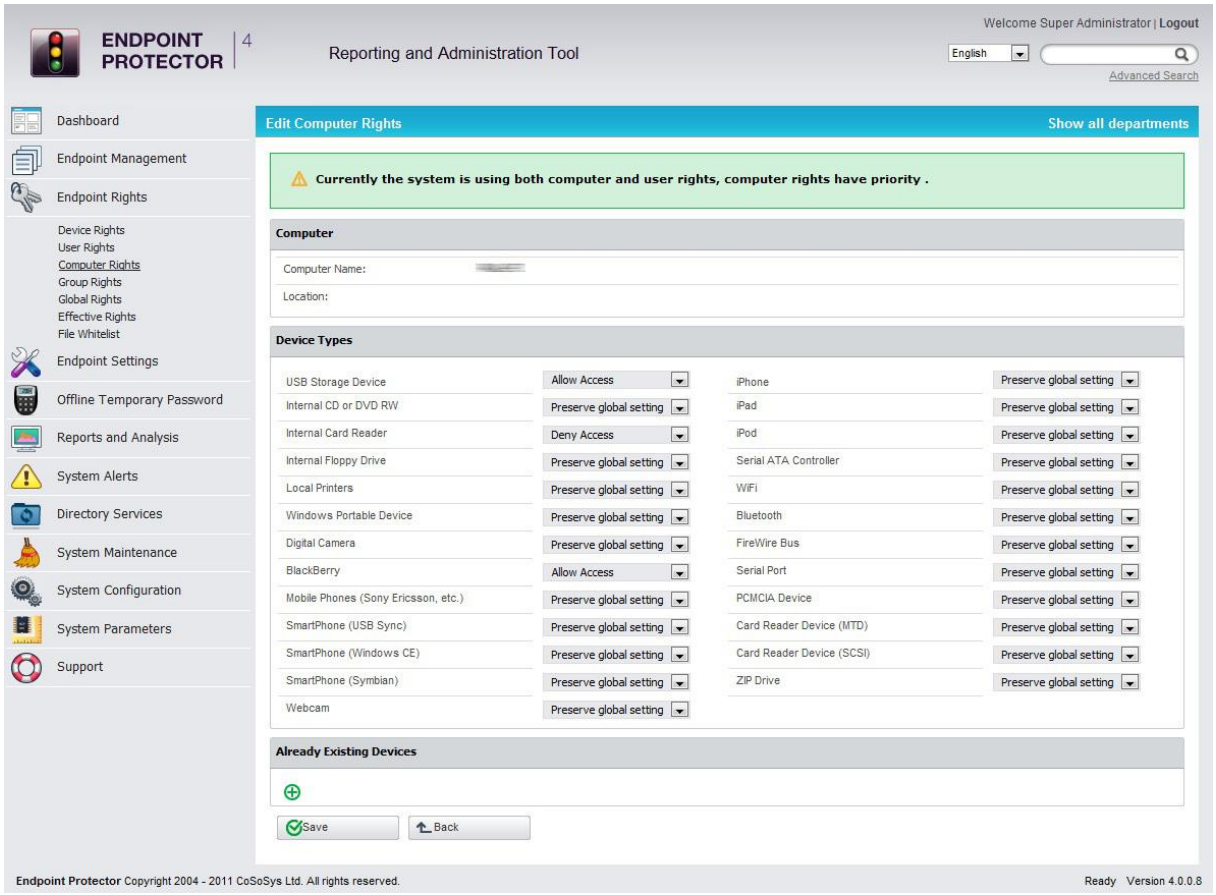
4.2. User Rights

This module is built around the user, allowing administrators to manage rights of access to devices per users.



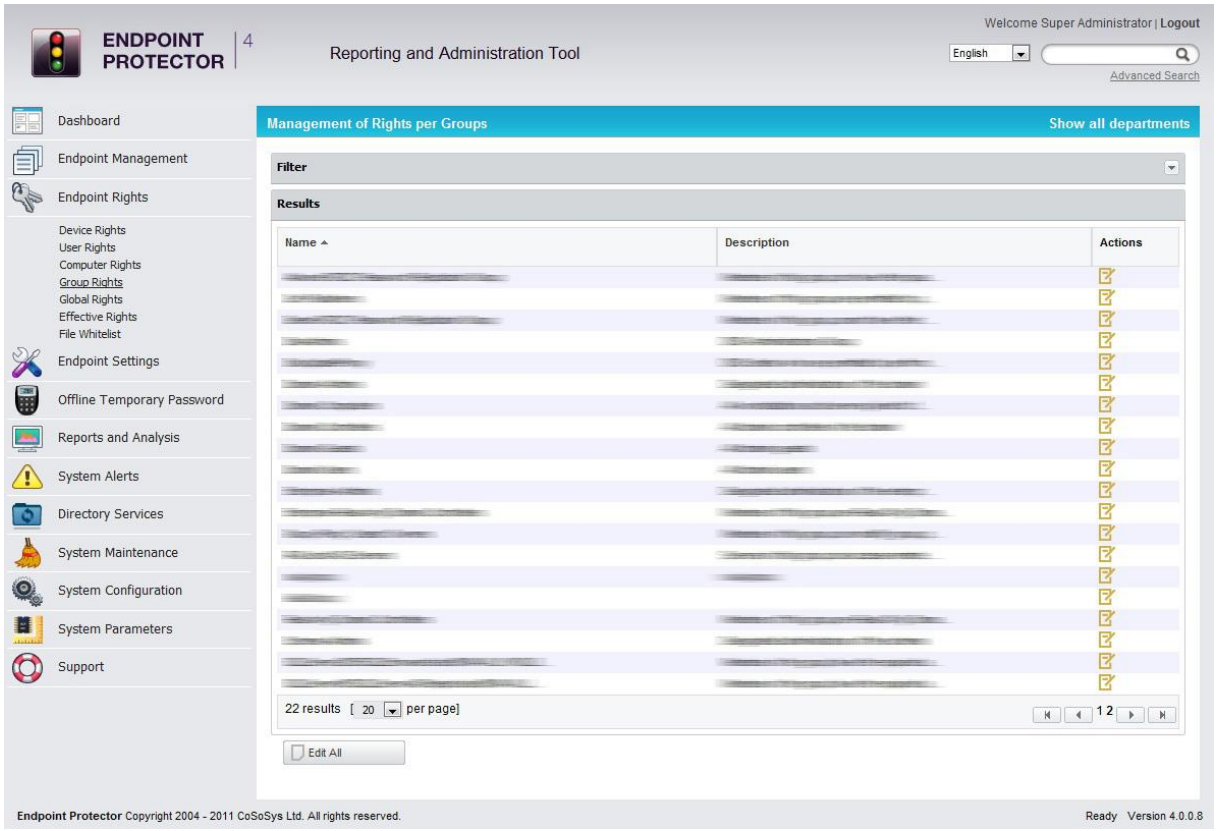
4.3. Computer Rights

This module will allow administrators to specify what device types and also what specific device(s) can be accessible from a single or all computers.



4.4. Group Rights

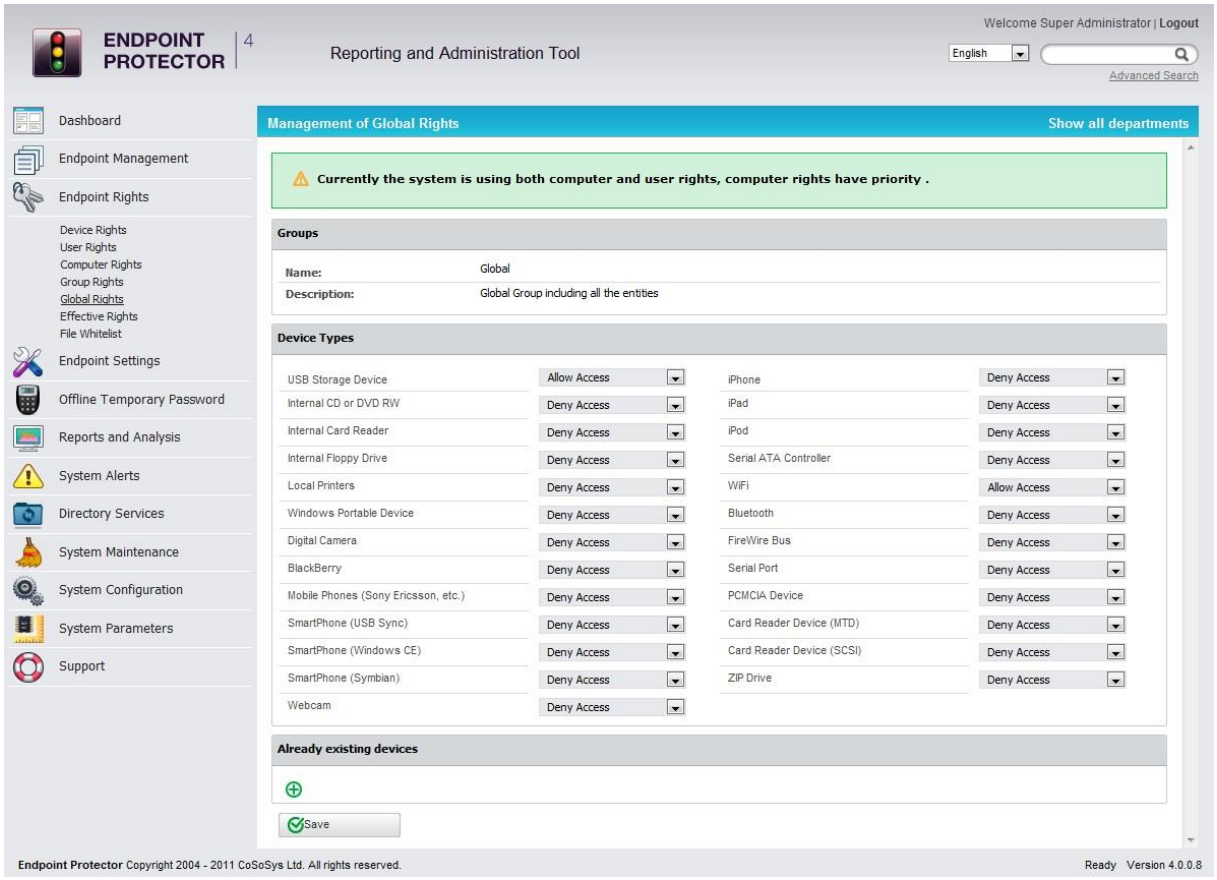
This module is similar to the previous one, only difference is that the rights here are applied to a group instead of a single computer.



The administrator can use the "Edit All" action here to edit rights for all groups at once.

4.5. Global Rights

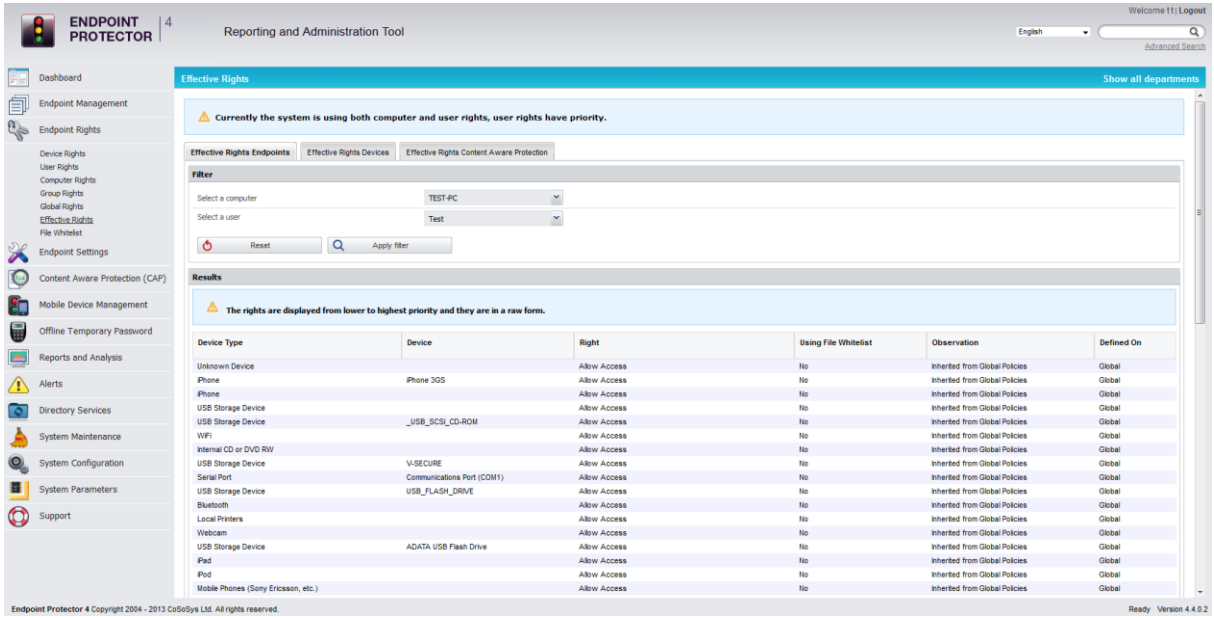
This module applies rights to computers in the entire system.



4.6. Effective Rights

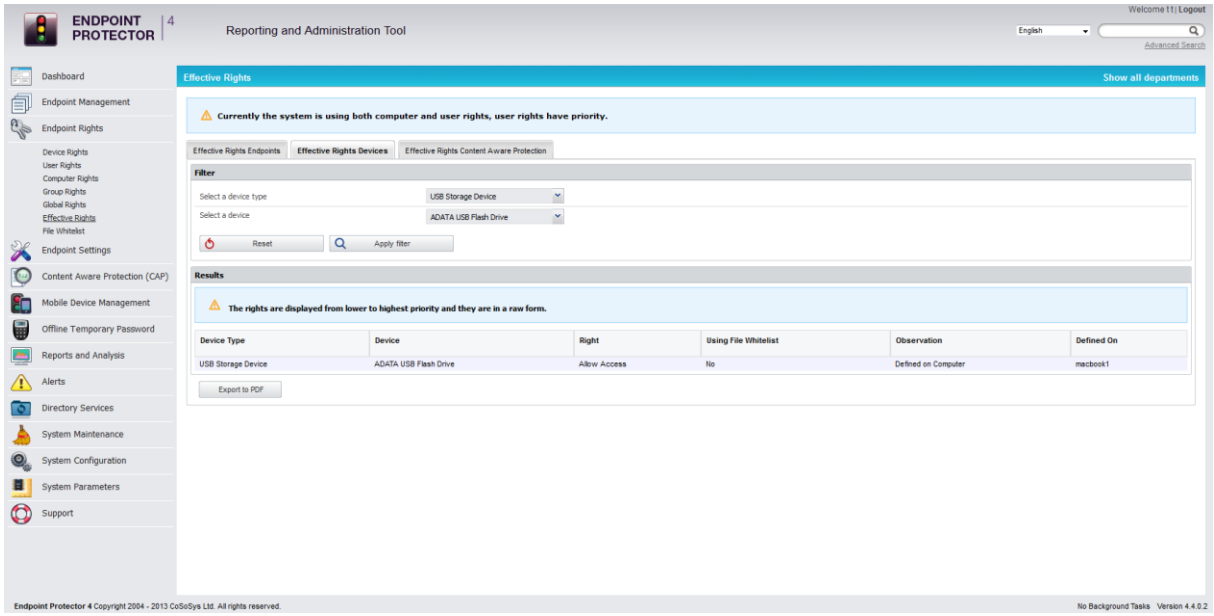
4.6.1. Effective Rights for Endpoints

This module displays the rights applied for all device types at that moment in time for the entire system or a specific user / computer.



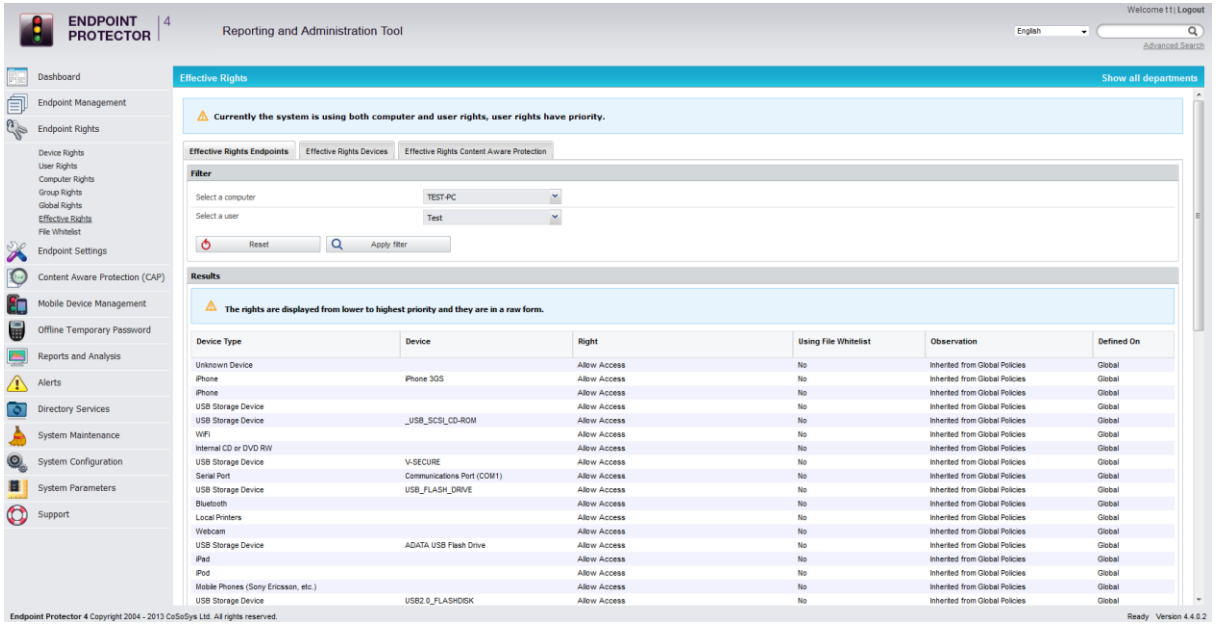
4.6.2. Effective Rights for Devices

This module displays the rights applied for the selected device.



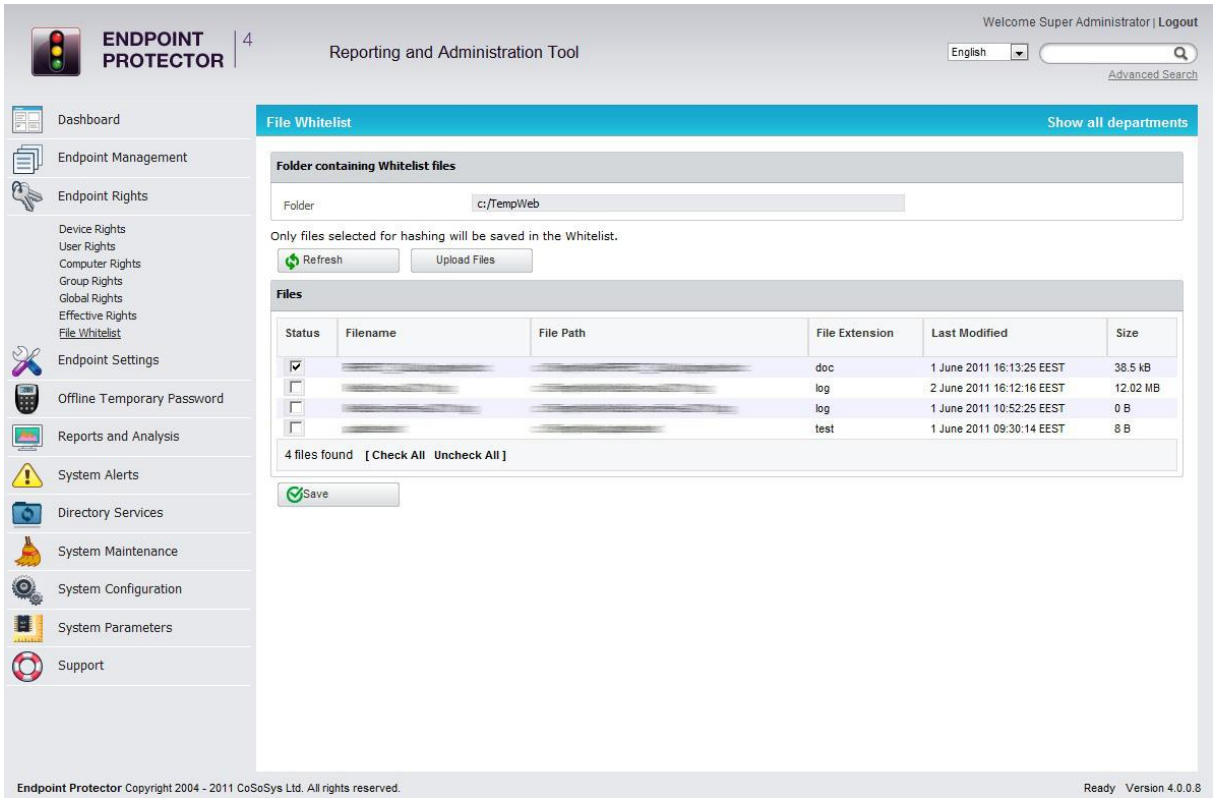
4.6.3. Effective Rights for Content Aware Protection

This module displays the Content Aware Protection rules on a specific user/computer at that time.


ENDPOINT PROTECTOR 4
Reporting and Administration Tool
Effective Rights
Show all departments
Currently the system is using both computer and user rights, user rights have priority.
Effective Rights Endpoints
Effective Rights Devices
Effective Rights Content Aware Protection
Filter
Results
The rights are displayed from lower to highest priority and they are in a raw form.

4.7. File Whitelist

This module allows the super administrator to control the transfer of only authorized files to previously authorized portable storage devices.



The super administrator can manage exactly what files can be copied to removable devices, and which cannot. In order to use this feature, the administrator must create a folder in which the authorized files will be kept and he must set this address in the "Folder" field.

After copying the required files into the previously created folder, he must simply press the "Refresh" button for a list to be generated.

Finally, he must check the box next to each file to enable it, and click the "Save" button. The files will be hashed and will receive permission to be copied.

This feature is only available to the Super Administrator user and cannot be modified by regular administrators.

Note!

This only works for outbound transfers. Files copied from external sources onto client (protected) computers will still be processed using the existing system policy.

5. Offline Temporary Password

5.1. Generating the Offline Temporary Password

This module allows the super administrator to generate a temporary password for:

- a specific device on a computer
- the Content Aware Protection feature on a computer
- the entire computer

It can be used when there is no network connection between the client computer and the Server.

Note!

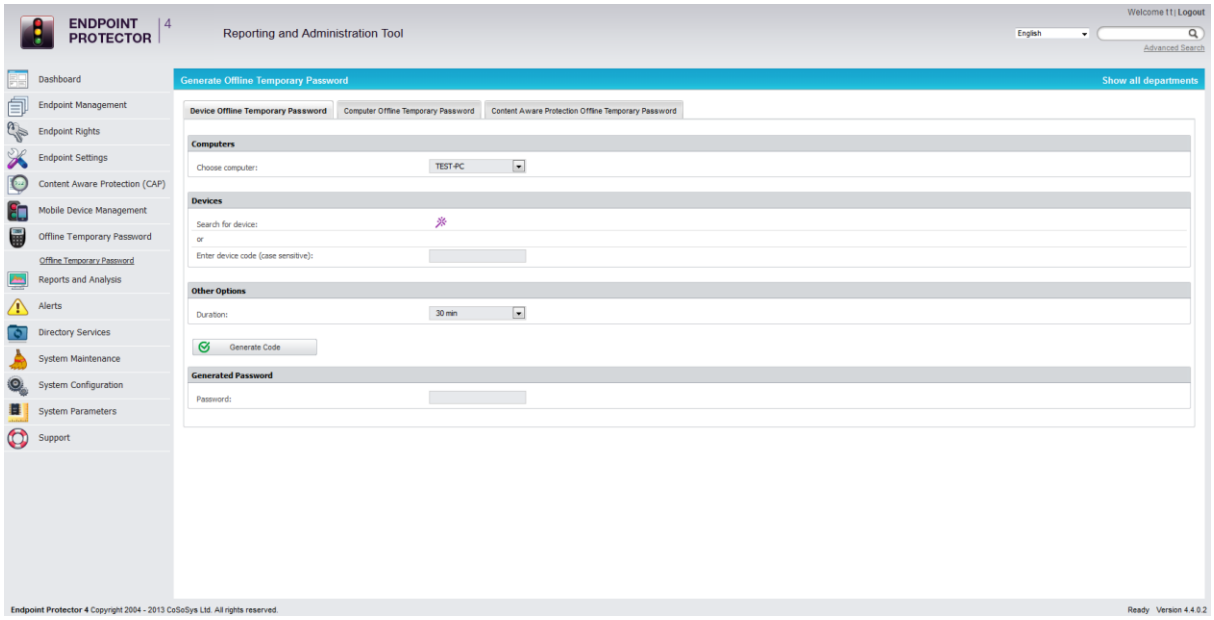
Once a device is temporarily authorized, any other rights/settings saved afterwards for this device will not take immediate effect, until the time period is passed and the connection with the Server is re-established.

A password is unique for a certain device and time period. In conclusion, the same password cannot be used for a different device or for the same device twice.

The password will give permission to the device, computer or sensitive data transfer for the specified amount of time.

The time intervals which can be selected are: 30 minutes, 1 hour, 2 hours, 4 hours, 8 hours, 1 day, 2 days, 5 days, 14 days and 30 days.

5.2. Device Offline Temporary Password

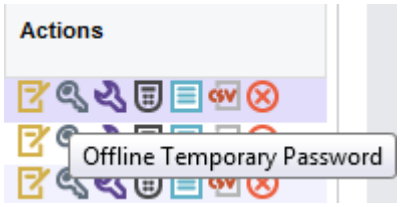


The administrator can either search for an existing device using the search wizard

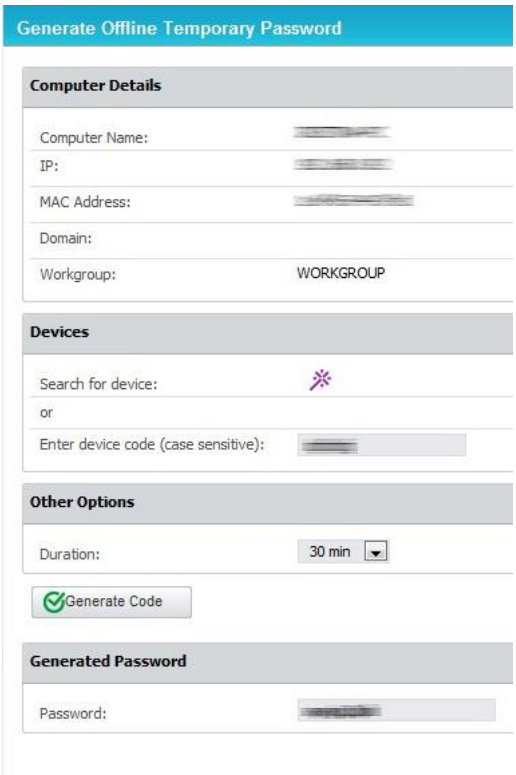
or, in case the device is not already in the database, he can introduce the device code communicated by the client user (see paragraph 5.5).

After selecting the duration, the password will be generated by clicking "Generate Code" button.

Another way to generate a password is by right clicking on a managed computer or device (from the Endpoint Management tab) and select the "Offline Temporary Password" action.

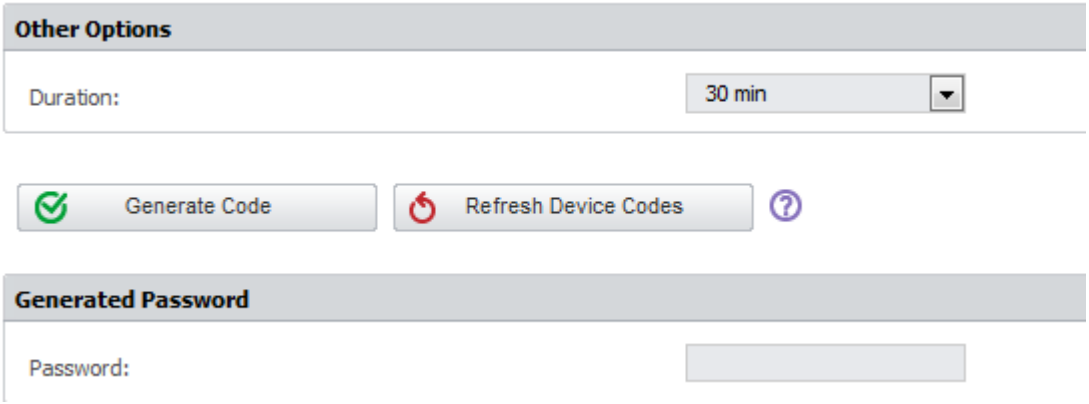


Once selected, generating a password can be done according to the details filled in, as per the image below:

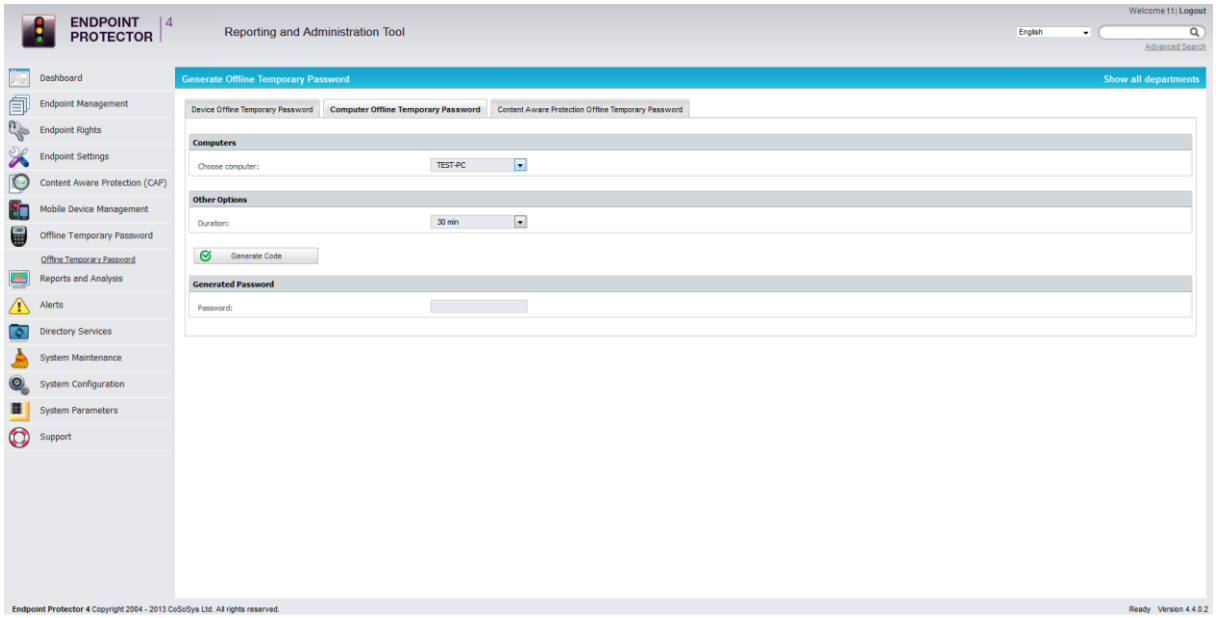


The obtained password will be communicated to the user for temporarily allowing his specific device.

With the "Refresh Device Codes" option, the Administrator can verity the authenticity of a given device code if it was previously listed in the Endpoint Management -> Devices list.

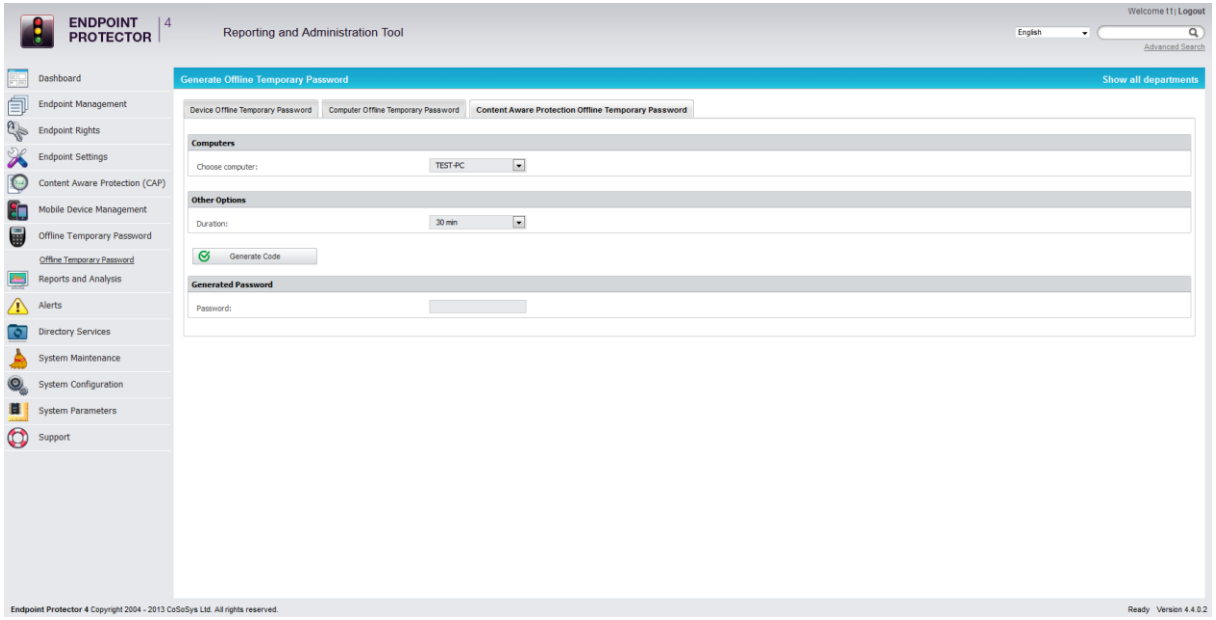


5.3. Computer Offline Temporary Password



The administrator can allow the use of all the endpoints on an offline computer. He does this by generating a Computer Offline Temporary Password. After selecting the computer and duration, the password will be generated by clicking on the "Generate Code" button. The obtained password will be communicated to the user for temporarily allowing the use of all the endpoints as explained in paragraph 5.5.

5.4. Content Aware Protection Offline Temporary Password

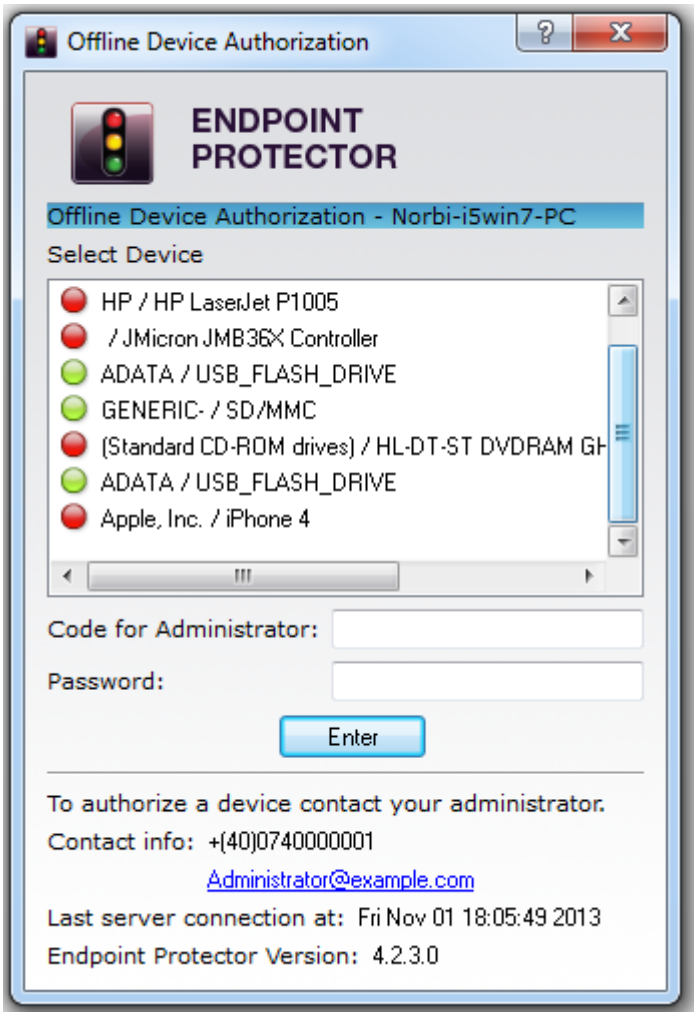


The administrator can allow the transfer of sensitive data on an offline computer. He does this by generating a Content Aware Protection Offline Temporary Password. After selecting the computer and duration, the password will be generated by clicking on "Generate Code" button. The obtained password will be communicated to the user for temporarily allowing transfer of sensitive data as explained in paragraph 5.5.

5.5. Offline Device, Computer and Content Aware Protection Authorization

In order to select a device and enter a password, the user needs to click on the Endpoint Protector icon from the system tray.

The user will select the device from the list and contact the administrator at the displayed contact information.



The user will tell the administrator the code for the device and the administrator will tell the user the password, after generating it on the Server (see above paragraph for password generation).

The password will be inserted in the correspondent field and applied by clicking "Enter".

For Computer and Content Aware Protection authorization the administrator will tell the user the password he previously generated.The user will simply enter it in the „Password" field and apply it by clicking „Enter".

5.6. Setting the Administrator Contact Information

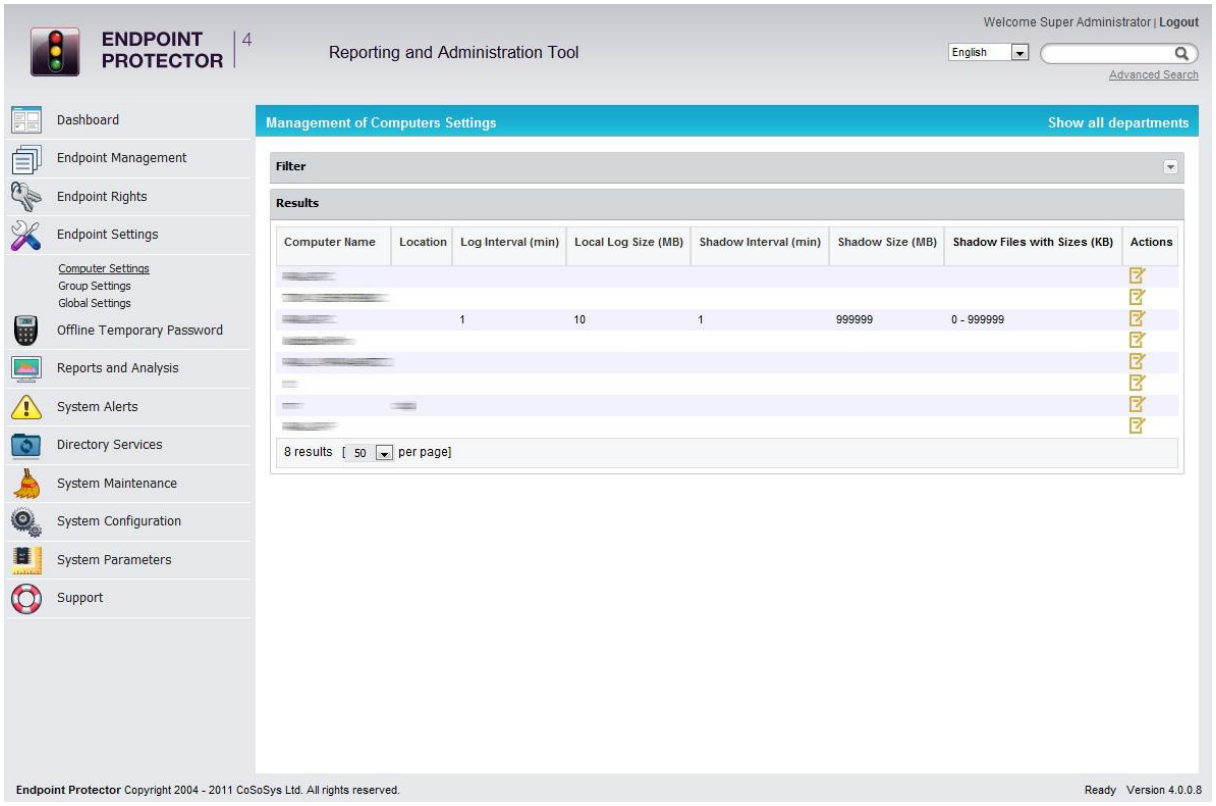
The Administrator contact information can be edited under "System Configuration" module, "System Settings" panel, edit "Main Administrator Contact Details", then click "Save".

Main Administrator Contact Details
Phone:
+(40)0740000001
E-mail:
Administrator@example.com
*Note: This contact information is referring to Offline Temporary Password only! For Alerts, you must setup the e-mail address from System Administrators > Edit info.
Save

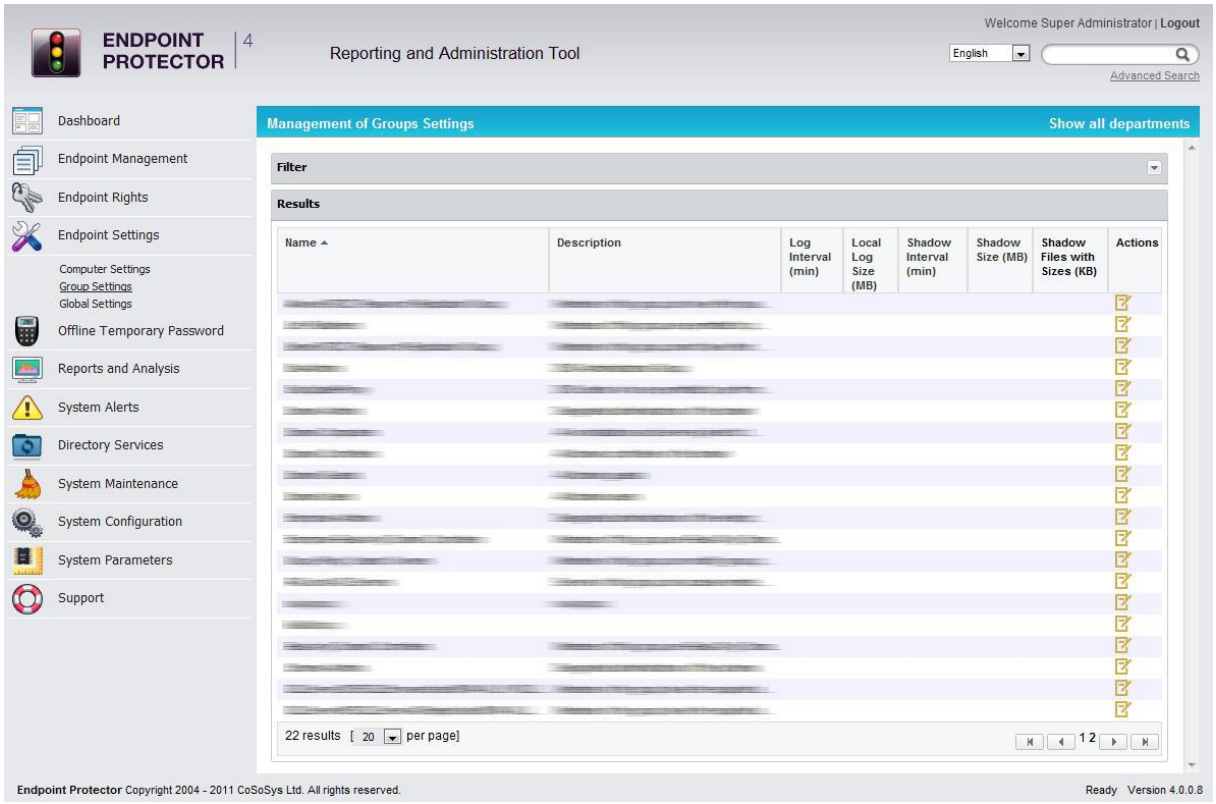
6. Endpoint Settings

The settings are attributes which are inherited. Settings are designed to be applied on computers, groups and globally (to all computers). The rule of inheritance is the following (from the most important to the least important):

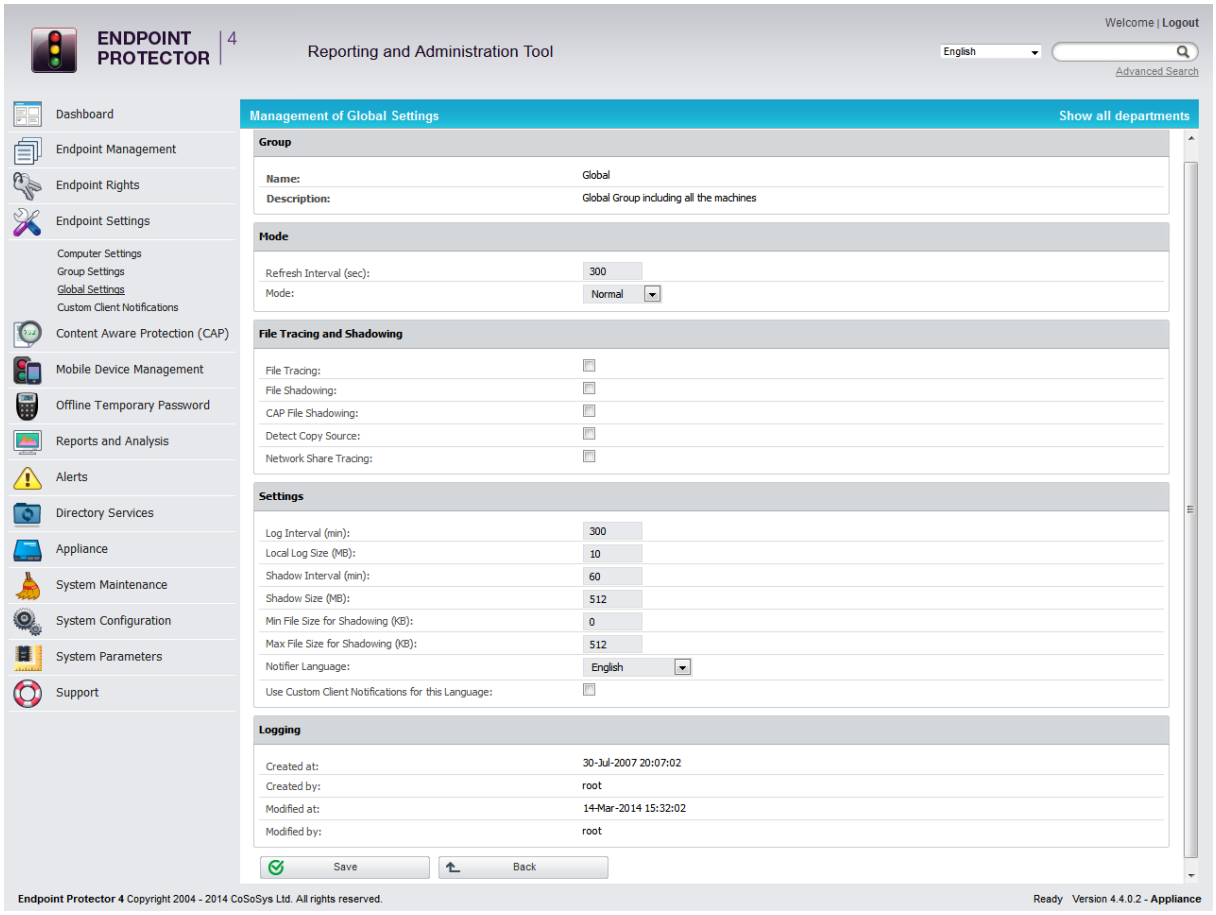
Computer Settings (settings applied to exactly one computer).

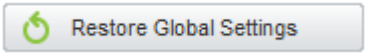


Group Settings (settings applied on a group).



Global Settings (settings applied for all the computers).



"Restore Global Settings" (

) button can be used to revert to a lower level of settings. Once this button is pushed the system will use the next level of settings.

Example: If the action is done on group settings, the entities in the group will use from that point onwards the global settings.

The settings and the rights for computers are sent to the client computer at an exact interval of time, set in this section.

Refresh Interval (in seconds) – represents the time interval at which the client will send a notification to the server with the intent to inform the server of its presence in the system. The server will respond by checking the settings and rights and updating them if needed, so the client can behave accordingly.

Log Upload Interval (in minutes) – represents the maximum time interval at which the client will send the locally stored log information to the server. This time interval can be smaller than the default value in case the log size is greater than the Local Log Size setting.

Local Log Size (in kilobytes) – represents the maximum size of the log which can be stored by the client on the client pc. If this value is reached then the client will send this information to the server.
This mechanism is optimal when a client computer has a lot of activity, because it will send the information very quickly to the server, so the administrator can be informed almost instantly about the activities on that computer.

Shadow Upload Interval (in minutes) – represents the maximum time interval at which the client will send the locally stored shadow information to the server.

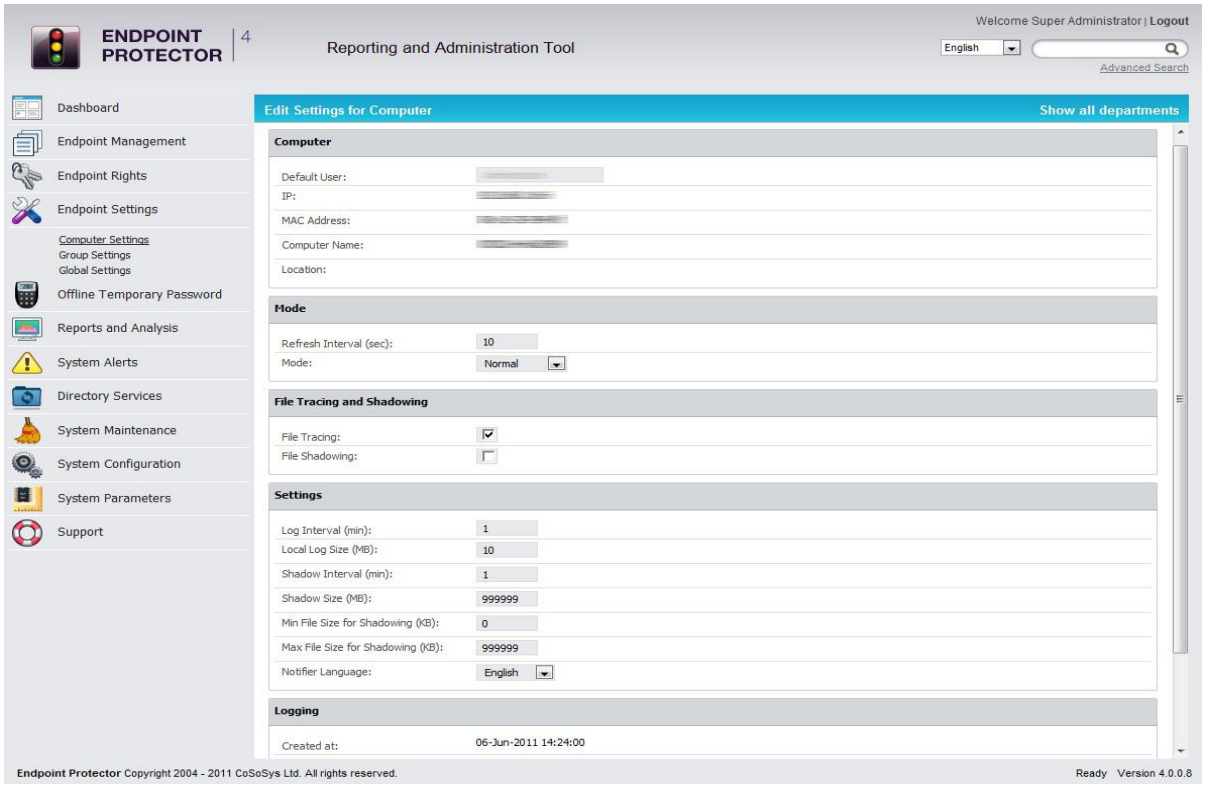
Local Shadow Size (in megabytes) – represents the maximum size of shadowed files stored by the client on a client PC. When this value is reached, the client will start overwriting existing files in order for it to not exceed the specified limit.

Minimum File Size for Shadowing (in kilobytes) – represents the minimum file size that should be shadowed. If a value is set here than files smaller in size than that value will not be shadowed.

Maximum File Size for Shadowing (in kilobytes) – represents the maximum file size that should be shadowed. If a value is set here, then files larger in size than that value will not be shadowed.

6.1. Computer Settings

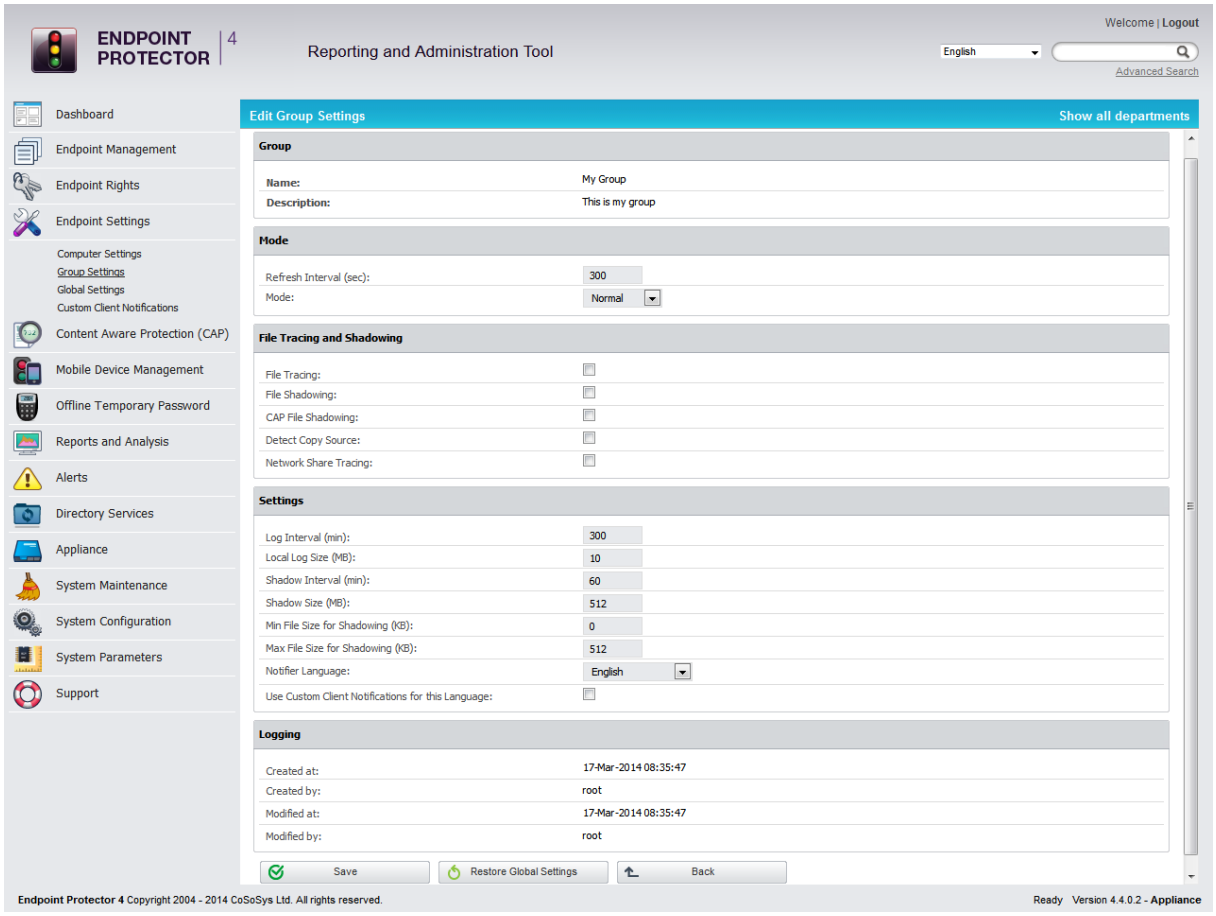
This module will allow the administrator to edit the settings for each computer.



Defining custom settings for all computers is not necessary, since a computer is perfectly capable of functioning correctly without any manual settings defined. It will do this by either inheriting the settings of a group it's in or, if not possible, the global settings, which are mandatory and exist in the system with default values from installation.

6.2. Group Settings

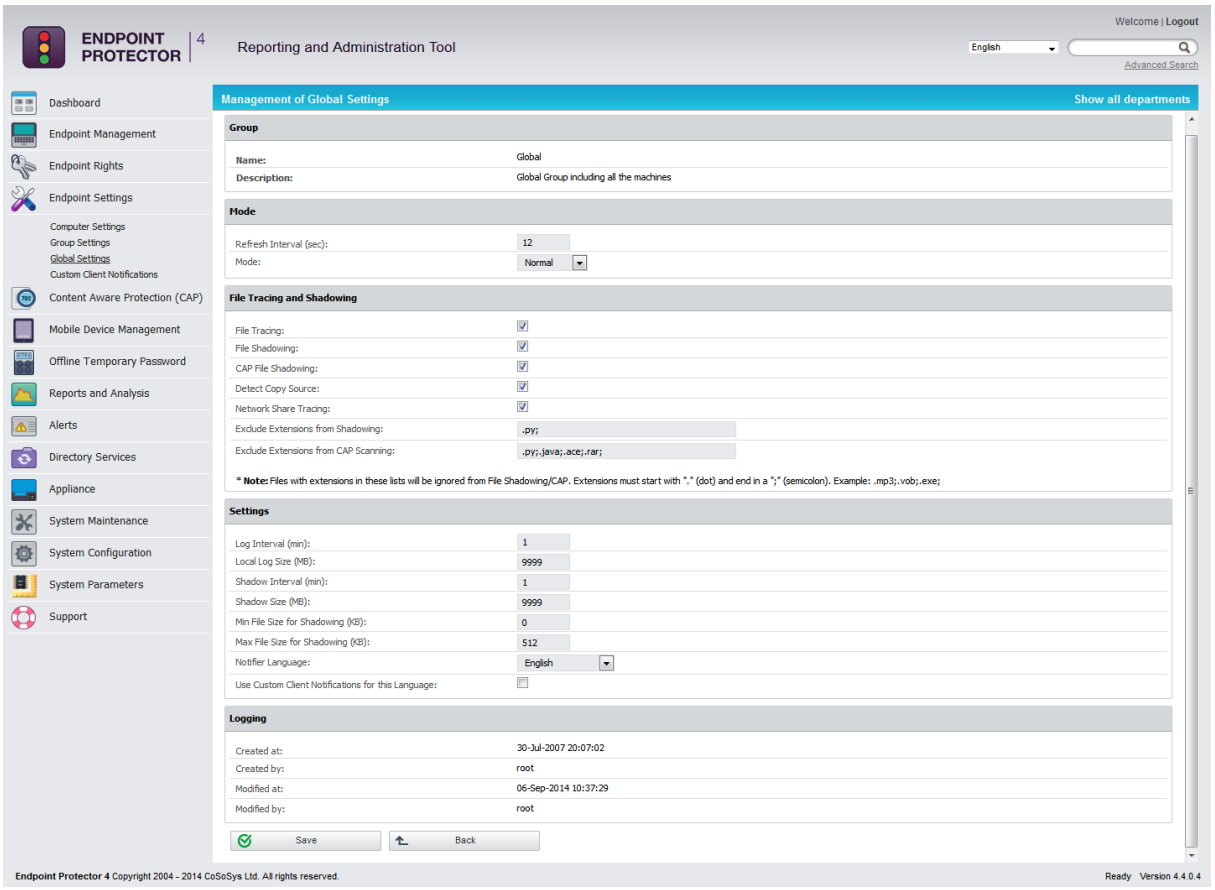
This module will allow the administrator to edit group settings.



We mentioned earlier that computers can be grouped so that editing of settings should be easier and more logical.

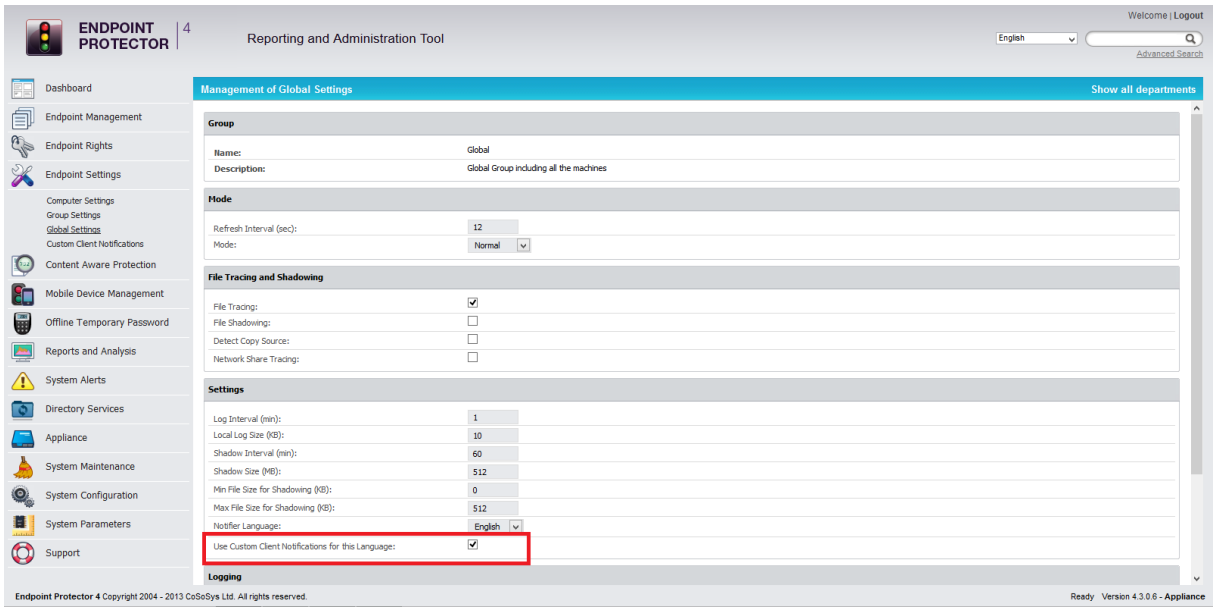
6.3. Global Settings

This module holds the global settings, which influence all computers within the system. If there are no settings defined for a computer, and it does not belong to a group, these are the settings it will inherit. If the computer belongs to a group, then it will inherit the settings of that group.



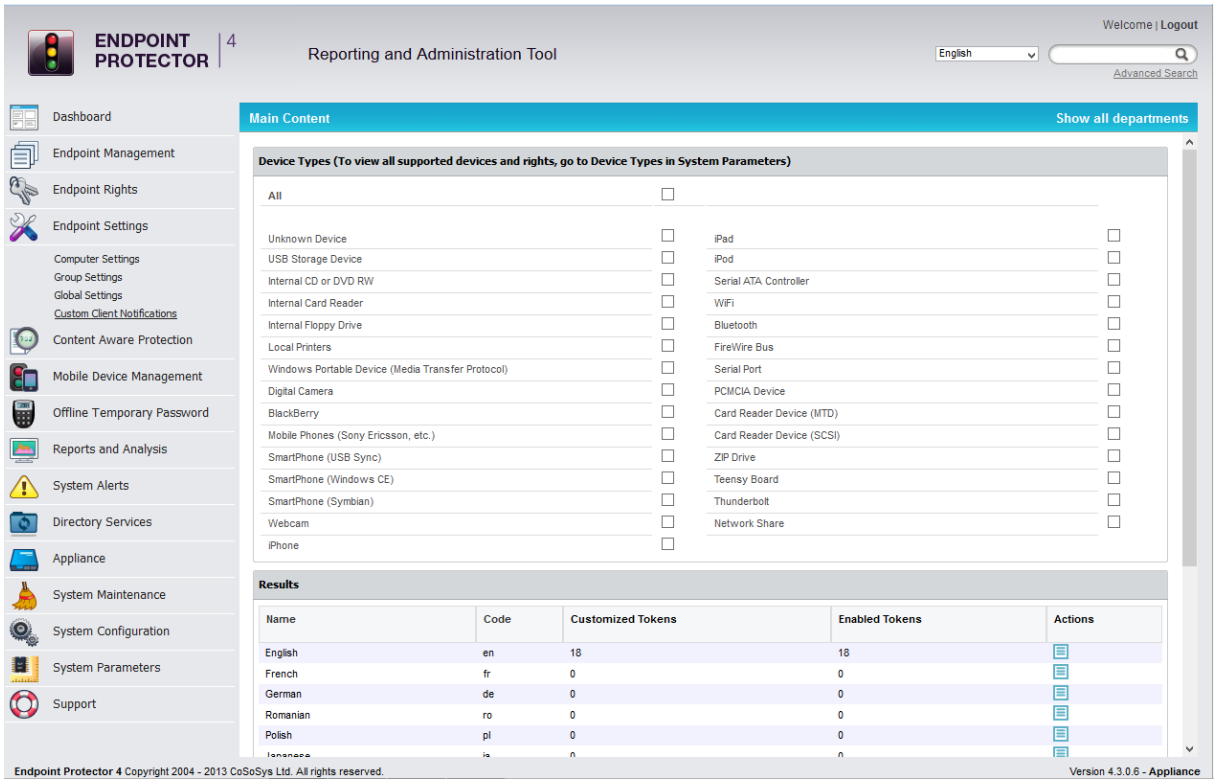
6.4. Custom Client Notifications

This feature allows the administrator to edit the notification messages that appear from the Agent of Endpoint Protector, for all available languages. Custom Client Notifications can be globally enabled from the Endpoint Settings tab. It can be individually checked on computers or groups.

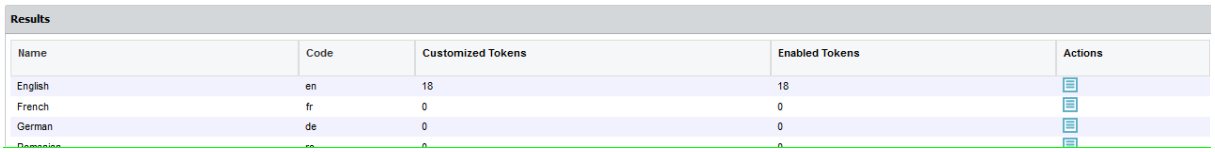


The administrator will have three options for each device type in part: to leave the default messages, to customize the message or to hide the message.

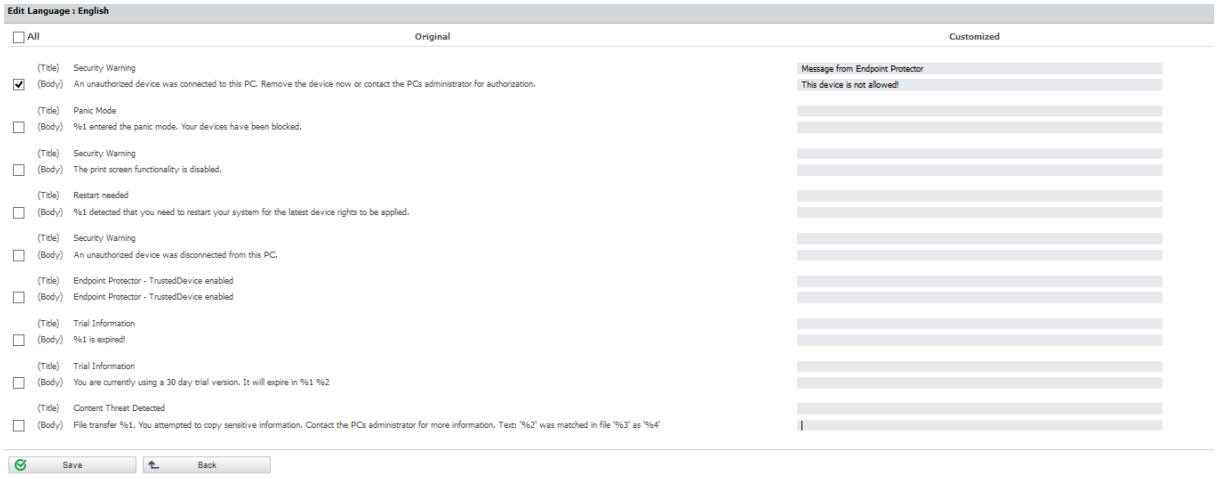
The administrator can select from the Device Types fields the devices types on which he wants the settings to be applied. The editable languages are available in Results section.



To edit the messages for a specific language, click on Actions.



In this example below we set the message as “Message from Endpoint Protector – This device is not allowed!”


Edit Language : English
All
Original
Customized
(Title) Security Warning
(Body) An unauthorized device was connected to this PC. Remove the device now or contact the PCs administrator for authorization.
Message from Endpoint Protector
This device is not allowed!
(Title) Panic Mode
(Body) %1 entered the panic mode. Your devices have been blocked.
(Title) Security Warning
(Body) The print screen functionality is disabled.
(Title) Restart needed
(Body) %1 detected that you need to restart your system for the latest device rights to be applied.
(Title) Security Warning
(Body) An unauthorized device was disconnected from this PC.
(Title) Endpoint Protector - TrustedDevice enabled
(Body) Endpoint Protector - TrustedDevice enabled
(Title) Trial Information
(Body) %1 is expired!
(Title) Trial Information
(Body) You are currently using a 30 day trial version. It will expire in %1 %2
(Title) Content Threat Detected
(Body) File transfer %1. You attempted to copy sensitive information. Contact the PCs administrator for more information. Text: '%2' was matched in file '%3' as '%4'
Save
Back

Some administrators might want not to display some notifications, while showing others. This can be done by (not) ticking the box for the specific message.

6.5. File Tracing

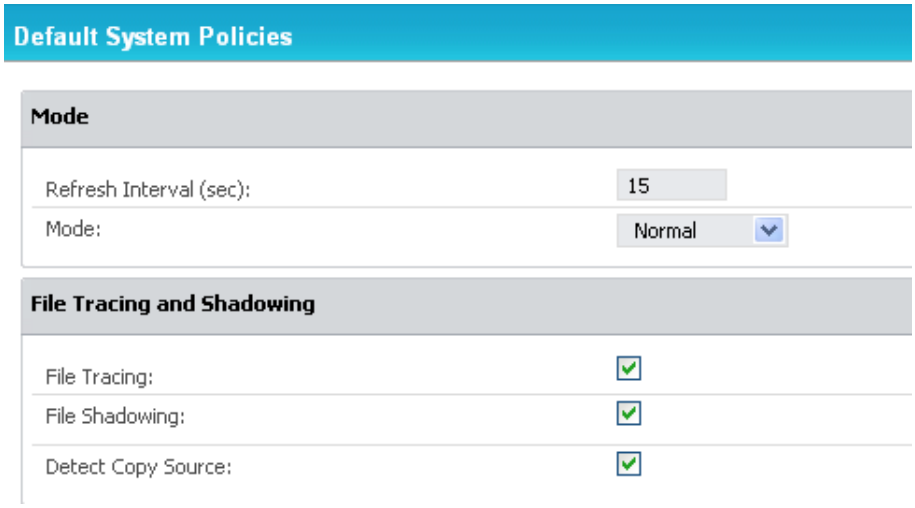
Endpoint Protector's file tracing feature allows monitoring of data traffic between protected clients and portable devices. It shows what files were copied, to which location, at what time and by which user. It also shows other actions that took place, such as file renamed, deleted, accessed, modified, etc.

Additionally, by selecting the option Detect Copy Source, the original file path for copied files to / from removable storage devices will be visible in Reports & Analysis > File Tracing under the File Name tab.
(ex. C:/Users/Me/Myfile.txt ->F:/Myfile.txt).

It is an essential feature for administrators since they can keep track of all data that's being transferred to and from devices. All traffic is recorded and logged for later auditing.

Administrators have the ability to enable or disable the file tracing feature. This can be done from within the Endpoint Protector Administration and Reporting Tool.

Access the "System Configuration" module and select "System Policies".



If you wish to disable the file tracing feature, simply uncheck the box next to it and click "Save".

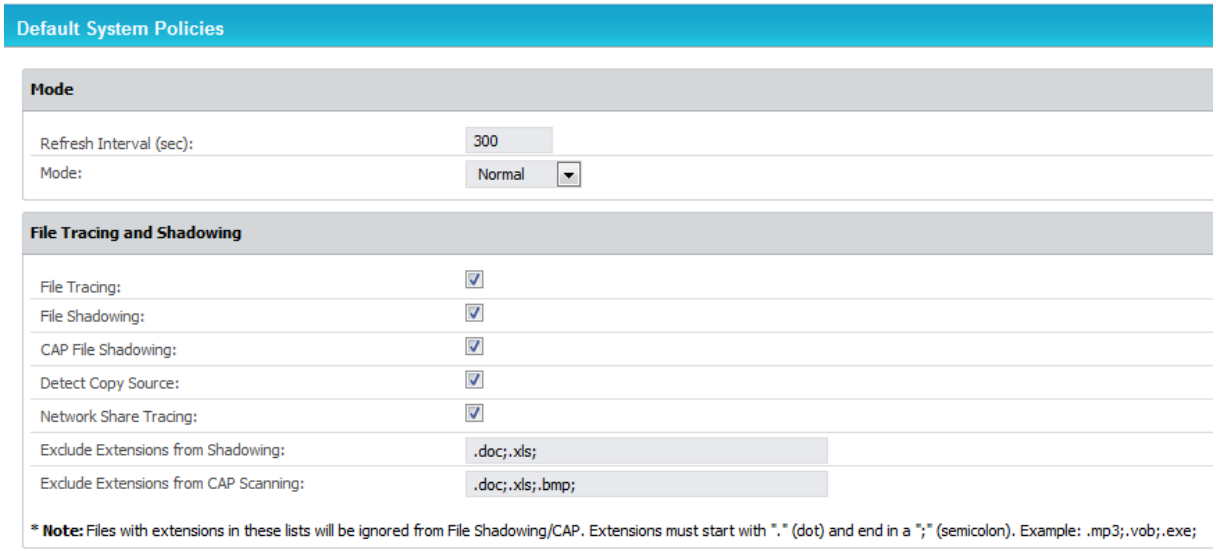
Note!

The option Detect Copy Source works only if File Tracing is activated.

6.6. File Shadowing

Endpoint Protector's File Shadowing feature works simultaneously together with File Tracing, creating exact copies of files accessed by users. The creation of shadow copies can be triggered by the following events: file copy, file write, and file read. Events such as file deleted, file renamed, etc. do not trigger the function.

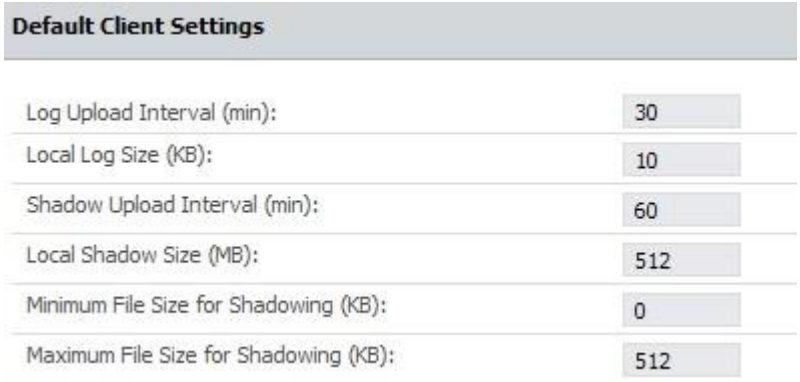
Same as File Tracing, Shadowing of files can be turned on or off, from the "System Configuration -> System Policies" module of the Endpoint Protector Reporting and Administration Tool. Please note, however, that this feature cannot be used without the File Tracing feature.



Note!

File Shadowing can be disabled for specific file types using the "Exclude Extensions from Shadowing" option.

Advanced settings such as minimum file size to be shadowed and shadowing upload interval can also be configured in this section.



Refresh Interval (in seconds) – Represents the time interval at which the client will send a notification to the server with the intent to inform the server of its presence in the system. The server will respond by checking the settings and rights and updating them if needed, so the client can behave accordingly.

Log Upload Interval (in minutes) – Represents the maximum time interval at which the client will send the locally stored log information to the server. This time interval can be smaller than the default value in case the log size is greater than the Local Log Size setting.

Local Log Size (in kilobytes) – represents the maximum size of the log which can be stored by the client on the client pc. If this value is reached then the client will send this information to the server.
This mechanism is optimal when a client computer has a lot of activity, because it will send the information very quickly to the server, so the administrator can be informed almost instantly about the activities on that computer.

Shadow Upload Interval (in minutes) – Represents the maximum time interval at which the client will send the locally stored shadow information to the server.

Local Shadow Size (in MB) – Represents the maximum size of shadowed files stored by the client on a client PC. When this value is reached, the client will start overwriting existing files in order for it to not exceed the specified limit.

Minimum File Size for Shadowing (in KB) – Represents the minimum file size that should be shadowed. If a value is set here than files smaller in size than that value will not be shadowed.

Maximum File Size for Shadowing (in KB) – Represents the maximum file size that should be shadowed. If a value is set here, then files larger in size than that value will not be shadowed.

The shadow directory can be selected from the "System Configuration" module under the "System Settings" tab.

Since shadow size can reach large amounts, we strongly recommend that a separate, large capacity Hard Disk is used for shadow storage.

Note!

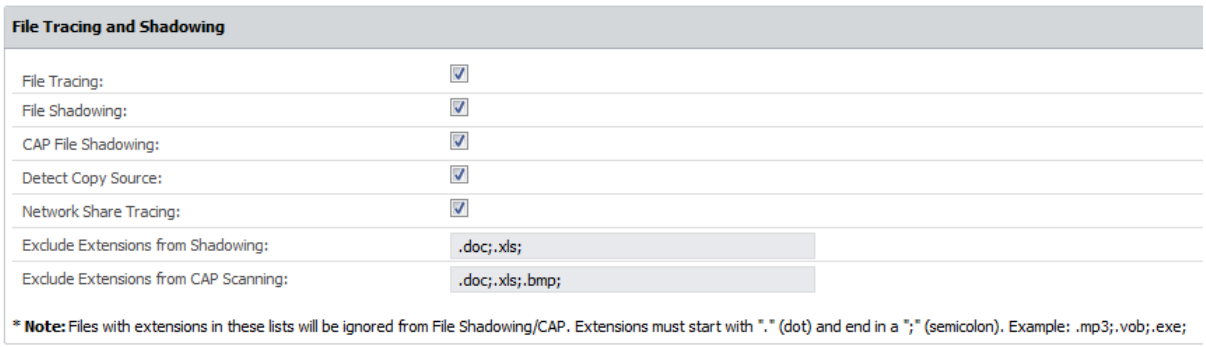
Shadowing Files can be delayed due to network traffic and Endpoint Protector Settings for different computers or file sizes. Shadowed files are usually available after a few minutes.

For large base installations (such as 250-1000 endpoints) we strongly advise to activate File Shadowing for up to 15% of your appliance (virtual or hardware) total endpoint capacity. (E.g. for an A1000 Hardware Appliance, File Shadowing should be set to maximum of 150 endpoints for optimal performance).

6.7. CAP File Shadowing

Endpoint Protector's File Shadowing feature works together with Content Aware Protection, creating exact copies of confidential files transferred by users. The creation of shadow copies can be triggered by the following events: content threat detected, content threat blocked.

CAP Shadowing can be turned on or off, from the "System Configuration -> System Policies" module of the Endpoint Protector Reporting and Administration Tool. Please note, however, that this feature is of no use without the Content Aware Protection feature.

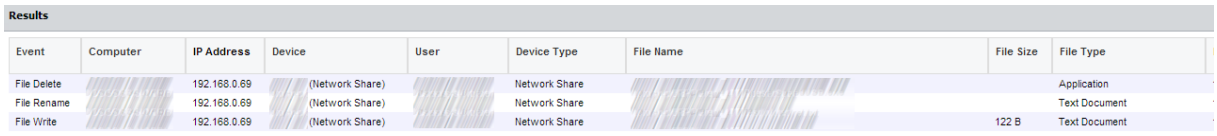

File Tracing and Shadowing
File Tracing:
File Shadowing:
CAP File Shadowing:
Detect Copy Source:
Network Share Tracing:
Exclude Extensions from Shadowing:
.doc;.xls;
Exclude Extensions from CAP Scanning:
.doc;.xls;.bmp;
* Note: Files with extensions in these lists will be ignored from File Shadowing/CAP. Extensions must start with "." (dot) and end in a ";" (semicolon). Example: .mp3;.vob;.exe;

Note!

CAP File Shadowing can be disabled for specific file types using the "Exclude Extensions from CAP Scanning" option.

6.8. Network Share Tracing

Endpoint Protector's network share tracing feature allows monitoring of data traffic between protected clients and other computers on the local network they are connected to. It shows what files were copied, to which location, at what time and by which user. It also shows other actions that took place, such as file written, renamed and deleted. The logs will be available in the "Reports & Analysis > File Tracing" Tab. Under the "device name" the computer on the network that receives the file will appear, followed in brackets by "Network Share" information.

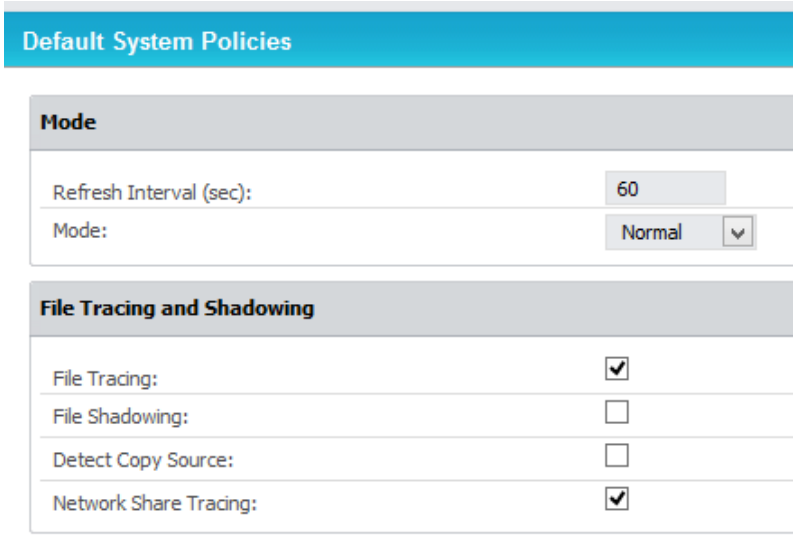


Additionally, by selecting the option Detect Copy Source, the original file path for copied files to / from removable storage devices will be visible in Reports & Analysis > File Tracing.

Administrators have the ability to enable or disable the file tracing feature. This can be done within the Endpoint Protector Administration and Reporting Tool.

Access the "System Configuration" module and select "System Policies".

In order to activate Network Share Tracing you need as a precondition to have also File Tracing enabled.



If you wish to disable the network share tracing feature, simply uncheck the box next to it and click "Save".

Note!

For large base installations (such as 250-1000 endpoints) we strongly advise to activate Network Share Tracing for up to 15% of your appliance (virtual or hardware) total endpoint capacity. (E.g. for an A1000 Hardware Appliance, Network Share Tracing should be set to maximum of 150 endpoints for optimal performance).

The option Network Share Tracing works only if File Tracing is activated as well. However, Network Share Tracing should be used at a minimum level for optimal performance.

7. Content Aware Protection

This module allows the administrator to setup and enforce strong content filtering policies for selected users, computers, groups or departments and take control over the risks posed by accidental or intentional file transfers of sensitive company data, such as:

- Personally Identifiable Information (PII): social security numbers (SSN), driving license numbers, E-MAIL addresses, passport numbers, phone numbers, addresses, dates, etc.
- Financial and credit card information: credit card numbers for Visa, MasterCard, American Express, JCB, Discover Card, Dinners Club, bank account numbers etc.
- Confidential files: sales and marketing reports, technical documents, accounting documents, customer databases etc.

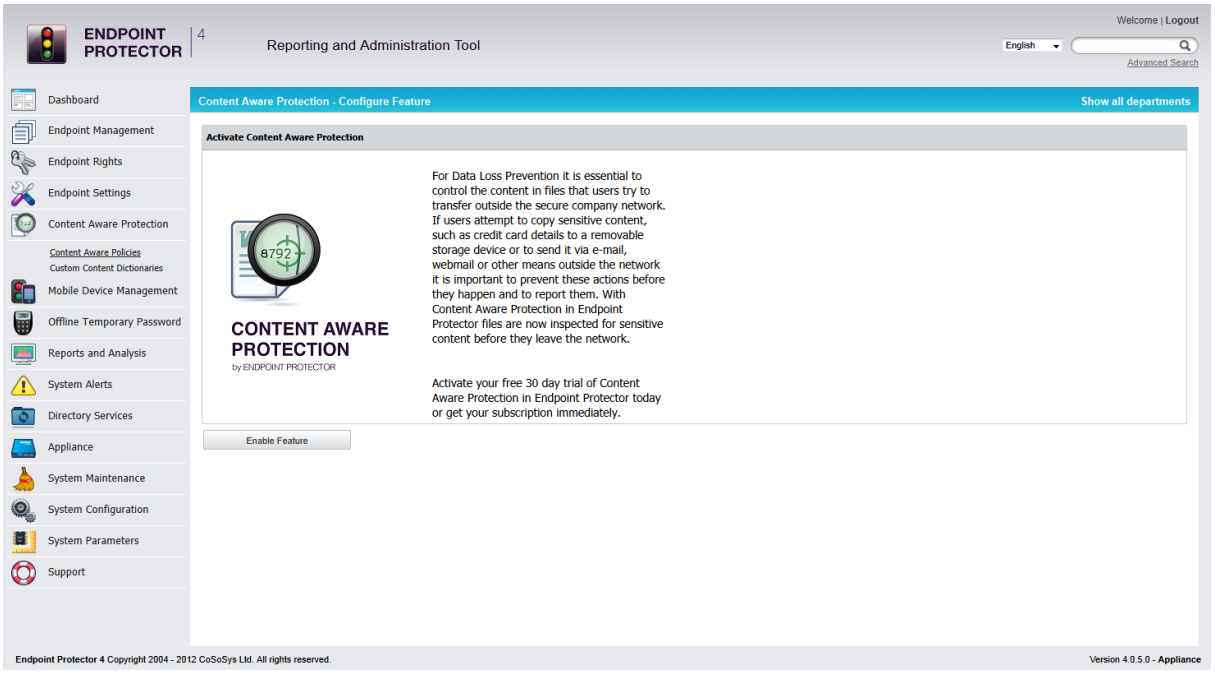
To prevent sensitive data leakage, Endpoint Protector closely monitors all activity at endpoints and other exit ways:

- Transfers on portable storage and other media devices (USB Drives, external hard-disks, CDs, DVDs, SD cards etc.), either directly or through encryption software (e.g. EasyLock)
- Transfers on local networks
- Transfers via Internet (E-MAIL clients, file sharing application, Web Browsers, Instant Messaging, Social Media)
- Transfers to the cloud (iCloud, Google Drive, Dropbox, Microsoft SkyDrive)
- Transfers through Copy & Paste / Cut & Paste
- Print screens

7.1. Activation of Content Aware Protection

Content Aware Protection comes as an optional feature with Endpoint Protector that requires a yearly-based separate subscription to be able to use it. The feature is displayed as deactivated inside the Endpoint Protector Reporting and Administration tool.

After a subscription is created, the Content Aware Protection feature can be enabled by simply selecting the Content Aware Protection option from the left-side menu and clicking on the Enable Feature button. The Content Aware Protection feature and all its options will be then activated for your system.


ENDPOINT PROTECTOR
4
Reporting and Administration Tool
Welcome | Logout
English
Advanced Search
Dashboard
Endpoint Management
Endpoint Rights
Endpoint Settings
Content Aware Protection
Content Aware Policies
Custom Content Dictionaries
Mobile Device Management
Offline Temporary Password
Reports and Analysis
System Alerts
Directory Services
Appliance
System Maintenance
System Configuration
System Parameters
Support
Content Aware Protection - Configure Feature
Show all departments
Activate Content Aware Protection
8792
CONTENT AWARE PROTECTION
by ENDPOINT PROTECTOR
For Data Loss Prevention it is essential to control the content in files that users try to transfer outside the secure company network. If users attempt to copy sensitive content, such as credit card details to a removable storage device or to send it via e-mail, webmail or other means outside the network it is important to prevent these actions before they happen and to report them. With Content Aware Protection in Endpoint Protector files are now inspected for sensitive content before they leave the network.
Activate your free 30 day trial of Content Aware Protection in Endpoint Protector today or get your subscription immediately.
Enable Feature
Endpoint Protector 4 Copyright 2004 - 2012 CoSoSys Ltd. All rights reserved.
Version 4.0.5.0 - Appliance

Note!

The Content Aware Protection feature requires separate licensing, in addition to the Endpoint Protector license for Device Control.

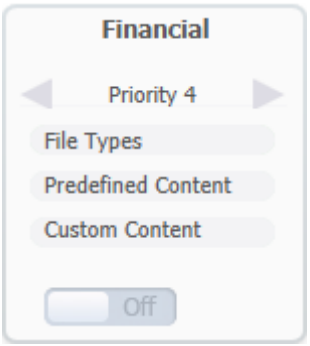
7.2. Content Aware Policies

Content Aware Policies are sets of rules for sensitive content detection and blocking enforced on selected network entities (users, computers, groups, departments).

A content aware policy is made up of four elements:

- Policy Type: defines for which type of OS the policy applies, Windows or Macintosh
- Policy Action: defines the type of action to be performed: reporting of sensitive content detection or blocking and reporting of sensitive content transfers
- Policy Filter: specifies the content to be detected, including: file type filtering, predefined content filtering and custom content filtering
- Policy Control Points: establishes the transfer destinations to be monitored

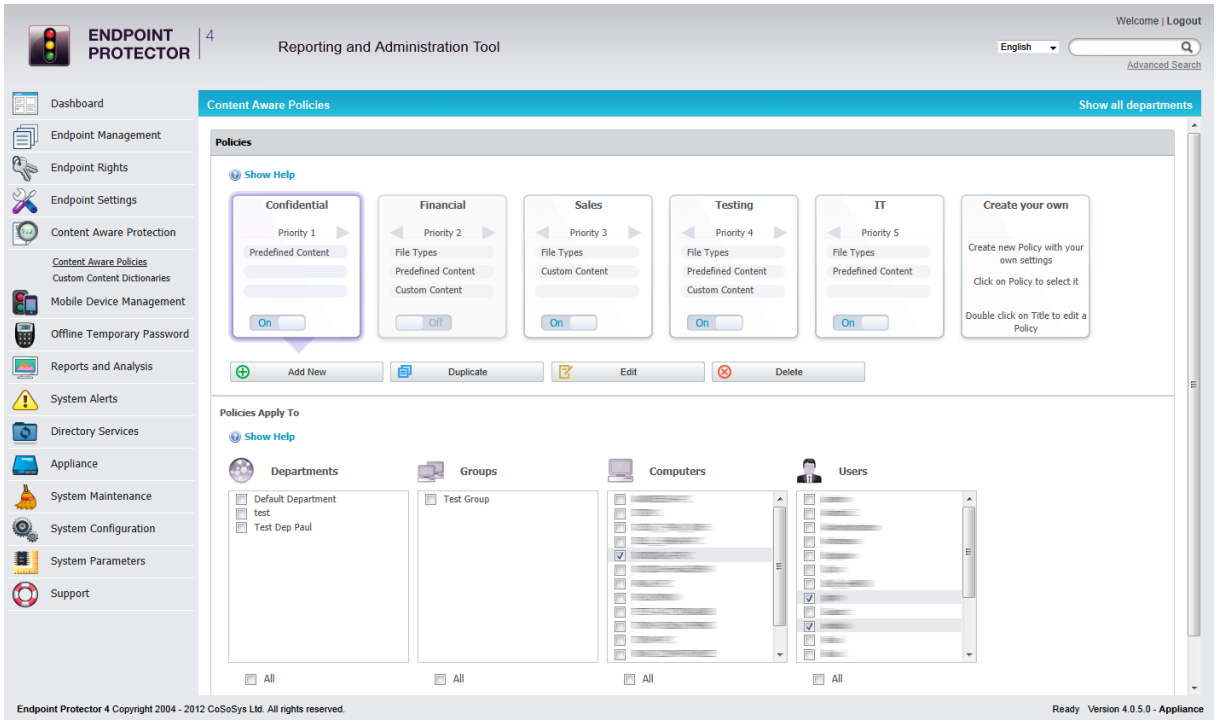
For example, a policy can be setup for the Financial Department of the company to block Excel reports sent via E-MAIL or to report all transfers of files containing personally identifiable and financial information (e.g. credit card numbers, E-MAILS, phone numbers, social security numbers etc.).



Additionally, each company can define its own sensitive content data lists as Custom Content Dictionaries corresponding to their specific domain of activity, targeted industry and roles. To ease this task, the Content Aware Protection module comes with a predefined Custom Content Dictionary that covers the most used sets of confidential terms and expressions.

Exactly like for Device Control policies, the Content Aware policies continue to be enforced on a computer even after it is disconnected from the company network.

The administrator can easily create and manage Content Aware Policies application inside the network from the Content Aware Protection -> Content Aware Policies submenu option.



The available actions are: **Add New**, **Duplicate**, **Edit** and **Delete**. A new policy can be created also by clicking on the "Create your own" policy icon. An existing policy can be edited also by double-clicking the upper part of the policy icon.

By selecting a policy, the departments, groups, computers and users on which the selected policy applies, will be highlighted for an easier policy management. The administrator can then uncheck previously enabled entities for monitoring or check new ones. All the changes performed on the page are applied after clicking "Save".

7.2.1. Priorities for Content Aware Policies

One or more Content Aware Policy can be enforced on the same computer, user, group or department. To avoid any conflicts between the applied rules, a prioritization of policies is performed through a left-to-right ordering. The leftmost policy has the highest priority (Priority 1), while the rightmost policy has the lowest priority. Changing priorities for one or more policies can be performed by moving the policy to the right or to the left with a simple click on the left arrow for higher priority or on the right arrow for lower priority.

7.2.2. How Content Aware Policies Work

Content Aware Protection is a very versatile tool, where granular implementation of the desired actions regarding report and/or block and report of files can be performed.

A Content Aware Policy is a set of rules for reporting or blocking & reporting the selected information. All the other options left unchecked will be considered as Ignored by Endpoint Protector.

When applying two policies to the same PC, it is possible to block one type of file, for example PNG files, when they are uploaded through Mozilla Firefox, while with a second policy to report only PNG files when they are uploaded through Internet Explorer. In the same way it is possible to report only files that contain confidential words from a selected dictionary that are sent through Skype, while with the second policy to block the same files if they are sent through Yahoo Messenger. Similarly, it is possible to create combinations that block a file type or a file that contains predefined content/custom content/regular expression for one application, while letting it through and report it only for another.

The following rules are used in the application of one or more Content Aware Policies on a computer/user/group/department for each separately selected item (e.g. a specific file type, predefined information or a custom content dictionary):

Policy A with Priority 1	Policy B with Priority 2	Policy C with Priority 3	Endpoint Protector Action
IGNORED	IGNORED	IGNORED	Information will not be blocked or reported.
IGNORED	IGNORED	*REPORTED*	Information will be reported.
IGNORED	*REPORTED*	*REPORTED*	Information will be reported.
REPORTED	*REPORTED*	*REPORTED*	Information will be reported.
IGNORED	IGNORED	**BLOCKED**	Information will be blocked.
IGNORED	**BLOCKED**	**BLOCKED**	Information will be blocked.
BLOCKED	**BLOCKED**	**BLOCKED**	Information will be blocked.
IGNORED	*REPORTED*	**BLOCKED**	Information will be reported.
IGNORED	**BLOCKED**	*REPORTED*	Information will be blocked.
REPORTED	IGNORED	**BLOCKED**	Information will be reported.
BLOCKED	IGNORED	*REPORTED*	Information will be blocked.
REPORTED	**BLOCKED**	IGNORED	Information will be reported.
BLOCKED	*REPORTED*	IGNORED	Information will be blocked.

Attention!

The information left unchecked when creating a policy will be considered as Ignored by Endpoint Protector and **NOT AS ALLOWED**.

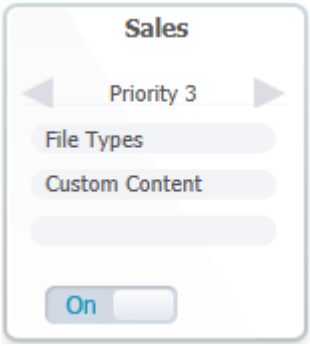
7.2.3. Types of Content Aware Policies

Depending on the selected content to detect, a policy can be classified in:

- **File Type Filter Policy**: detects/blocks all transfers of preselected file types, including preselected file types archived in zip files with no password protection
- **Predefined Content Policy**: detects/blocks all file transfers containing Credit Card and/or Personal Identifiable information
- **Custom Content Policy**: detects/blocks all file transfers containing terms from a preselected Custom Content Dictionary

Combined policies can be created by selecting several filter types for the same policy.

An example of a combined Content Aware Policy for the Sales Department to detect specific file types and custom terms is shown below.



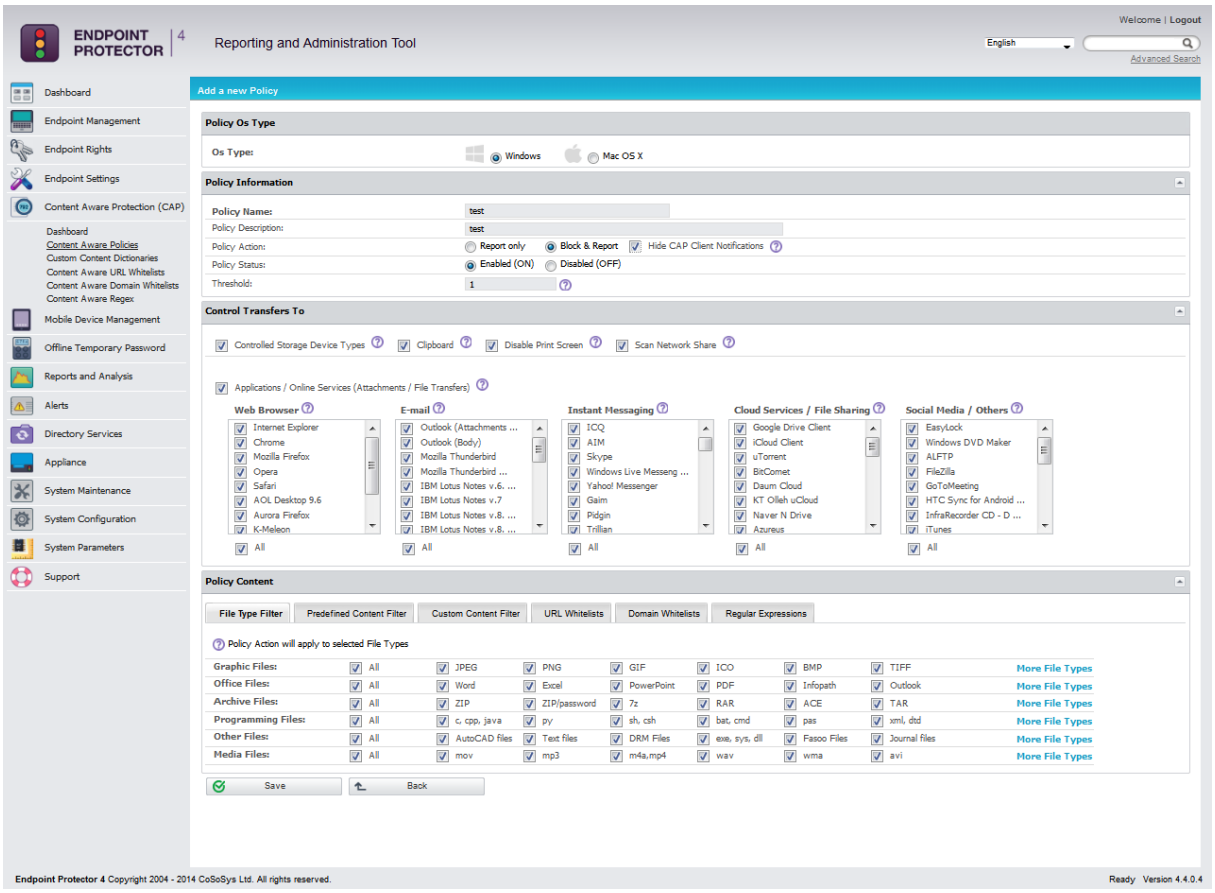
Depending on the selected content to monitor, the icon corresponding to the newly created policy will highlight the specific selected filters.

Note!

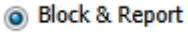
Content Aware Policies apply also to File Whitelist. This means that all files that were previously whitelisted will be inspected for sensitive content detection, reported and / or blocked according to the defined policy.

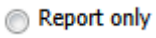
7.2.4. Setting up Content Aware Policies

To setup a Content Aware Policy, go to Content Aware Protection -> Content Aware Policies and click on the Create Your Own Policy icon or push the "Add Policy" button. This will open the Add a new Policy window, which will allow setting the parameters of the newly created policy.



A policy can be enforced to detect & report all transfers of sensitive content data and/or block all transfers:





Note!

The Block & Report action will block all file transfers on the selected network entity. We recommend using the Report only action initially to detect but not block data transfers. This way, no activity will be interrupted and you can gain a better view of data use across your network.

By default, data control is turned off. To activate the defined content rules, a newly created policy must be enabled (ON). The policy status can be changed later by using the simple ON/OFF switch from the policy icon:

Note!

An enabled (ON) Policy will be enforced only after selecting the network entities to be monitored.

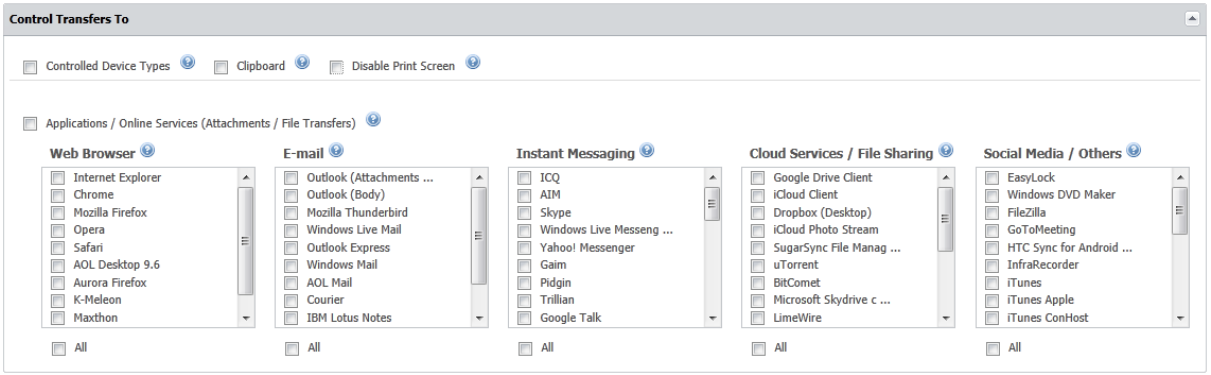
A powerful Content Aware Policy option consists of setting up a threshold number. A threshold is defined by the number of actions or events up to which the policy does not block a defined action. For example, suppose that you have set up a "Block & Report" policy on the transfer of Social Security Numbers on some types of Internet browsers. A threshold setup of two (2) will block all transfers on those browsers which contain two or more individual SSN numbers, but not one (1). A set value of two will permit and only report individual transfers of one single string of monitored sensitive information.

Note!

Enabling the threshold option will produce no effect when Policy Action is set on "Report Only".

The threshold option applies strictly on the "Predefined Content" filter of the Content Aware Protection module.

To complete the policy definition, the transfer destinations to be monitored must be selected and the content to be detected must be specified.



There are five main categories of transfer destinations to control:

- Controlled device types: comprises the list of all removable devices registered to Endpoint Protector.

Note!

For Controlled Device Types category, Endpoint Protector will monitor file transfers both to and from removable media.

- Clipboard: refers to all content captured through Copy & Paste and Cut & Paste operations

- Disable Print Screen: refers to the screen capture option
- Scan Network Share: refers to content uploaded to local networks
- Applications / Online Services (Attachments / File Transfers): comprises Web Browsers, E-MAIL Clients, IM, File Sharing, Social Media/Others.

Type	List of Applications
Web Browsers	Internet Explorer, Mozilla Firefox, Chrome, Opera, Safari, SeaMonkey, Maxthon, AOL Destop 9.6, K-Meleon, Aurora Firefox
E-MAIL Clients	Microsoft Office Outlook, Mozilla Thunderbird, Windows Live Mail, Outlook Express, Windows Mail, AOL Mail, Opera Mail, SeaMonkey Mail, Courier, IBM Lotus Notes, GroupWise Client
Instant Messaging	AIM, eBuddy, MySpace IM, ICQ, Google Talk, Skype, Windows Live Messenger, Yahoo! Messenger, mIRC, Trillian, MyChat, LingoWare, Chit Chat For Facebook, Nimbuzz, Facebook Messenger, Microsoft Communicator 2007, Facemoods, Gaim, LAN Chat Enterprise, OpenTalk, TurboIRC, WinSent Messenger, Pink Notes Plus, fTalk, XChat, ooVoo, TweetDeck, Pidgin Instant Messenger,NateOn Messenger, QQ International , Twhirl, Daum MyPeople
Cloud Services / File Sharing	Google Drive Client, iCloud, Dropbox, Microsoft SkyDrive, eMule, Kazaa, Shareaza, Morpheus, eDonkey, DC++, BitTorrent, Azureus, BitComet, uTorrent, iMesh, Daum Cloud, KT Olleh uCloud, Naver NDrive, Microsoft Skydrive client, Limewire, FTP Command, ownCloud client, Pogoplug Backup, Pruna P2P, Sendspace, Evernote, FileCloud Sync client
Social Media/Others	InfraRecorder, iTunes, Nokia PC Suite 2008 / 2011, Samsung Kies, Sony Ericsson PC Companion, TeamViewer, HTC Sync for Android phones, Total Commander, LogMeIn, EasyLock, GoToMeeting, Windows DVD Maker, FileZilla, ALFTP, GoToMeeting

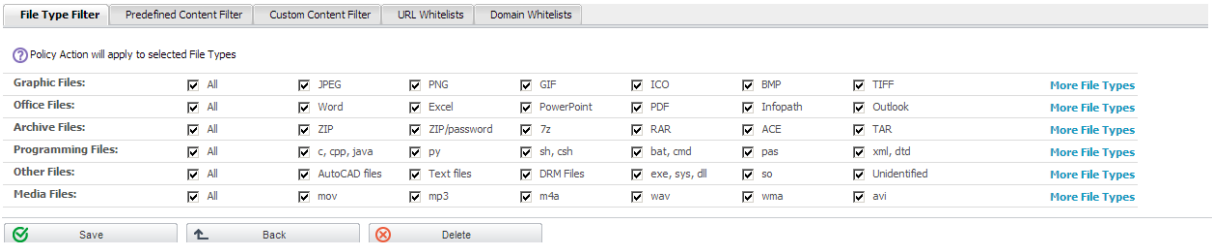
The last step in defining a new policy consists in selecting the content to detect from the three separate tabs for Content Filters.

The File Type Filter contains a list of supported file types grouped in six categories:

- Graphic Files: JPEG, PNG, GIF, ICO, BMP, TIFF, EPS, CorelDraw etc.
- Office Files: Word (DOC, DOCX), Excel (XLS, XLSX), PowerPoint (PPT, PPTX), PDF, Infopath (XSN), RTF, OneNote (ONE), Outlook (PST, OST) etc.
- Archive Files: ZIP, 7z, RAR, ACE, TAR etc.

- Programming Files: C, CPP, JAVA, PY, SH, CSH, BAT, CMD, PAS, XML, DTD TEX, F etc.
- Media Files: MP3, M4A, WAV, WMA, AVI, AIF, M3U, MPA etc.
- Other Files: EXE, SYS, DLL, SO etc.

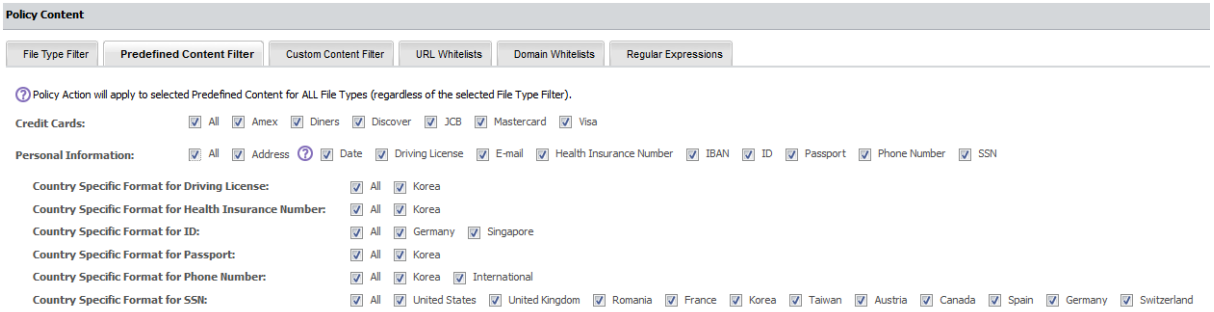
For each category, the most common file types are displayed. To be able to view and select more file types, click on the More File Types option at the end of each file type enumeration.


File Type Filter
Predefined Content Filter
Custom Content Filter
URL Whitelists
Domain Whitelists
Policy Action will apply to selected File Types
Graphic Files: All JPEG PNG GIF ICO BMP TIFF More File Types
Office Files: All Word Excel PowerPoint PDF Infopath Outlook More File Types
Archive Files: All ZIP ZIP/password 7z RAR ACE TAR More File Types
Programming Files: All c, cpp, java py sh, csh bat, cmd pas xml, dtd More File Types
Other Files: All AutoCAD files Text files DRM Files exe, sys, dll so Unidentified More File Types
Media Files: All mov mp3 m4a wav wma avi More File Types
Save
Back
Delete

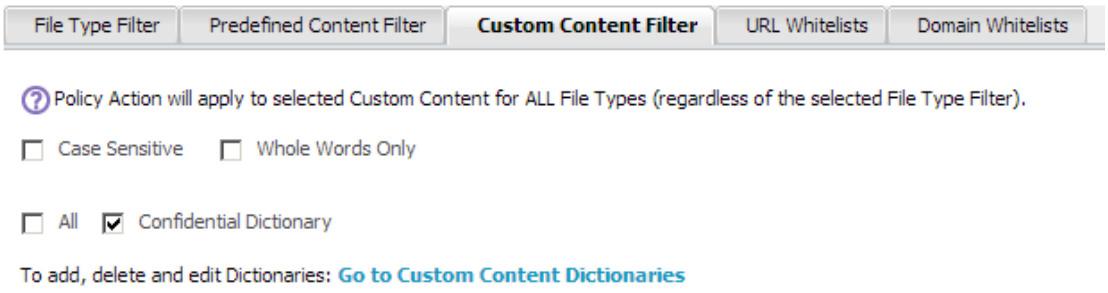
Note!

As many files (e.g. Programming Files) are actually .TXT files, we recommend more precaution when selecting this file type to avoid any undesired effects.

The "Predefined Content Filter" displays a list of predefined items to detect, from credit card information to Personal Identifiable Information. The Content Aware Protection module offers the option of Localization, meaning that you can select specific formats for a list of countries for information such as Driving License, ID, Phone Number and Social Security Number. By leaving unchecked this option, all formats will be detected by the Content Aware Protection agent.


Policy Content
File Type Filter
Predefined Content Filter
Custom Content Filter
URL Whitelists
Domain Whitelists
Regular Expressions
Policy Action will apply to selected Predefined Content for ALL File Types (regardless of the selected File Type Filter).
Credit Cards: All Amex Diners Discover JCB Mastercard Visa
Personal Information: All Address Date Driving License E-mail Health Insurance Number IBAN ID Passport Phone Number SSN
Country Specific Format for Driving License: All Korea
Country Specific Format for Health Insurance Number: All Korea
Country Specific Format for ID: All Germany Singapore
Country Specific Format for Passport: All Korea
Country Specific Format for Phone Number: All Korea International
Country Specific Format for SSN: All United States United Kingdom Romania France Korea Taiwan Austria Canada Spain Germany Switzerland

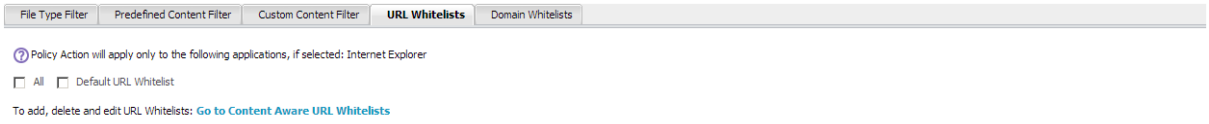
The "Custom Content Filter" displays a list of Content Aware dictionaries. By selecting one or more dictionaries, the Content Aware Protection agent will detect any occurrence of one, more or all terms contained in the Dictionary list.


File Type Filter
Predefined Content Filter
Custom Content Filter
URL Whitelists
Domain Whitelists
Policy Action will apply to selected Custom Content for ALL File Types (regardless of the selected File Type Filter).
Case Sensitive
Whole Words Only
All
Confidential Dictionary
To add, delete and edit Dictionaries: Go to Custom Content Dictionaries

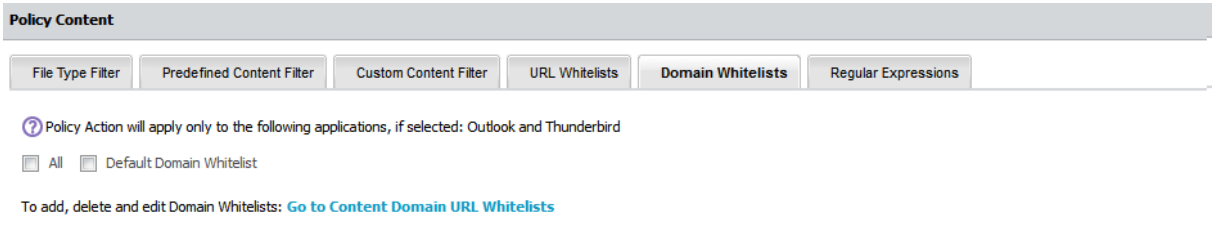
By checking the Case Sensitive option, the agent can differentiate the uppercase and lowercase letters when inspecting the content.

If the Whole Words Only option is marked, terms from the inspected content are detected only if they are an identical match with the ones that appear in the dictionary (e.g. „age" is in the Dictionary; variations like „aged", „agent", „agency" etc. won´t be reported/blocked).

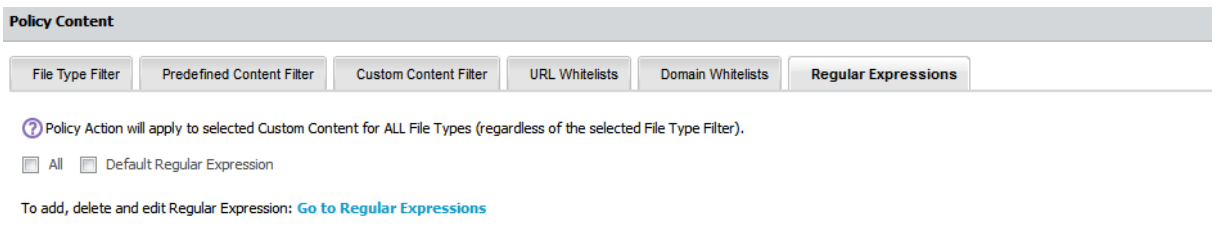
The "URL Whitelist" displays a list of URL whitelists. By selecting one or more whitelists, the Content Aware Protection agent will not scan uploads or attachments to the web addresses present in the whitelists. Whitelisting works for Internet Explorer.


File Type Filter
Predefined Content Filter
Custom Content Filter
URL Whitelists
Domain Whitelists
Policy Action will apply only to the following applications, if selected: Internet Explorer
All
Default URL Whitelist
To add, delete and edit URL Whitelists: Go to Content Aware URL Whitelists

The "Domain Whitelist" displays a list of domain whitelists. By selecting one or more whitelists, the Content Aware Protection agent will not scan mails sent to the recipients or domains present in the whitelists. Whitelisting works for Microsoft Outlook and Mozilla Thunderbird.


Policy Content
File Type Filter
Predefined Content Filter
Custom Content Filter
URL Whitelists
Domain Whitelists
Regular Expressions
Policy Action will apply only to the following applications, if selected: Outlook and Thunderbird
All
Default Domain Whitelist
To add, delete and edit Domain Whitelists: Go to Content Domain URL Whitelists

The "Regular Expressions" shows the list of the created regular expressions and the administrator can select up to five (5) expressions.


Policy Content
File Type Filter
Predefined Content Filter
Custom Content Filter
URL Whitelists
Domain Whitelists
Regular Expressions
Policy Action will apply to selected Custom Content for ALL File Types (regardless of the selected File Type Filter).
All
Default Regular Expression
To add, delete and edit Regular Expression: Go to Regular Expressions

Once a policy is created, it will be displayed inside the Policies List. To enforce a content aware policy inside the network, one must select the specific policy that they want to apply by clicking on it and check the corresponding boxes to the network entity on which they want to apply the content rules. If a Content Aware Policy was already enforced on a computer, user, group or department, when clicking on it, the corresponding network entities on which it was applied will be highlighted.

The administrator can be notified of each occurrence of an event described in a newly created policy by setting up a Content Aware alert for that specific policy from System Alerts -> Content Aware Alerts.

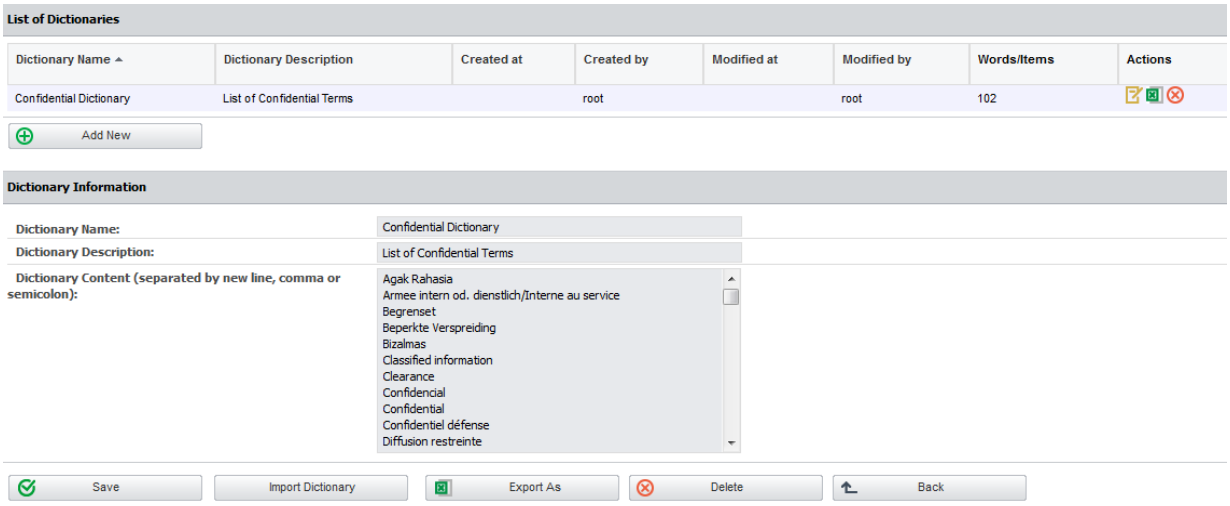
7.3. Custom Content Dictionaries

Custom Content Dictionaries are custom defined lists of terms and expressions to be detected as sensitive content by Endpoint Protector. The list of custom content dictionaries is available under Content Aware Protection -> Custom Content Dictionaries.

The available actions for each dictionary are: **Edit**, **Export Dictionary** and **Delete**.

A new dictionary can be created by clicking on the "Add New" button. To populate the content of a newly created dictionary, items of at least three characters might be entered either manually separated by comma, semicolon or new line or directly imported from an Excel file by pressing the Import Dictionary button.

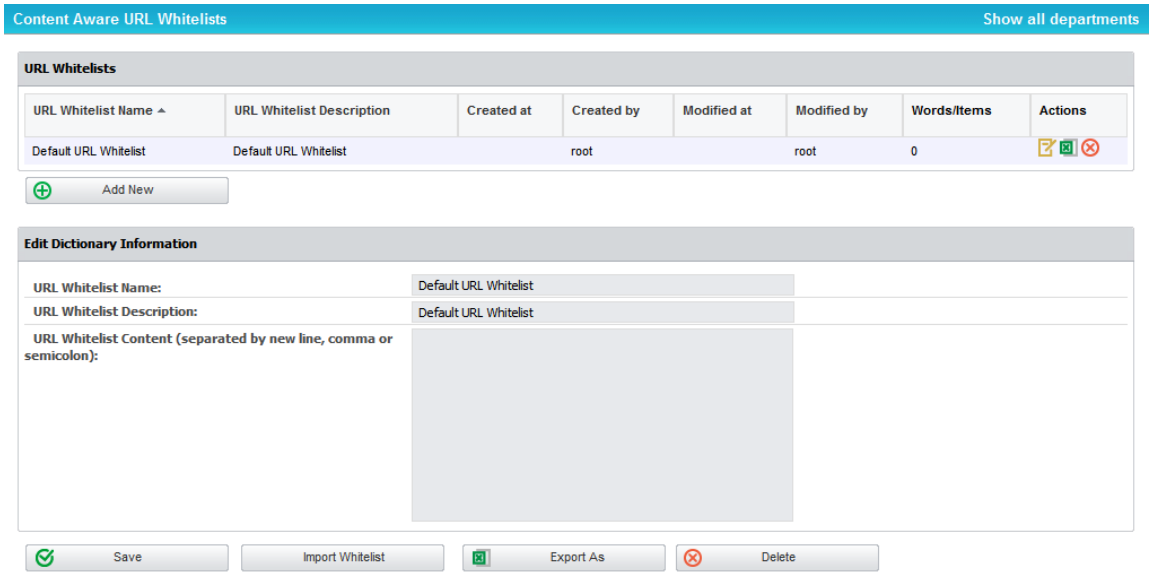
An example of a Custom Content Dictionary with financial terms is shown below:



Once a new dictionary is created, it will be automatically displayed inside the Custom Content tab when creating a new or editing an existing Content Aware Policy. The Content Aware Protection module comes with a predefined set of dictionaries.

7.4. Content Aware URL Whitelists

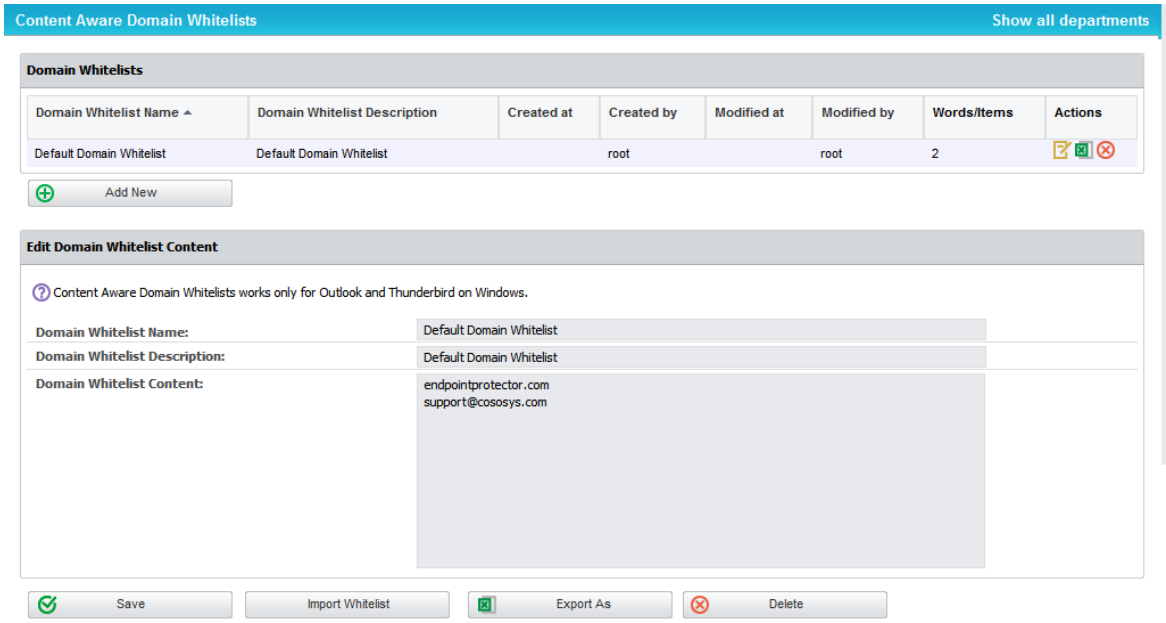
URL Whitelists are custom defined lists of web addresses where uploading of confidential information will be allowed by the Endpoint Protector. This feature works on Internet Explorer.



Once a new URL whitelist is added, it will be automatically displayed inside the URL Whitelists tab.

7.5. Content Aware Domain Whitelists

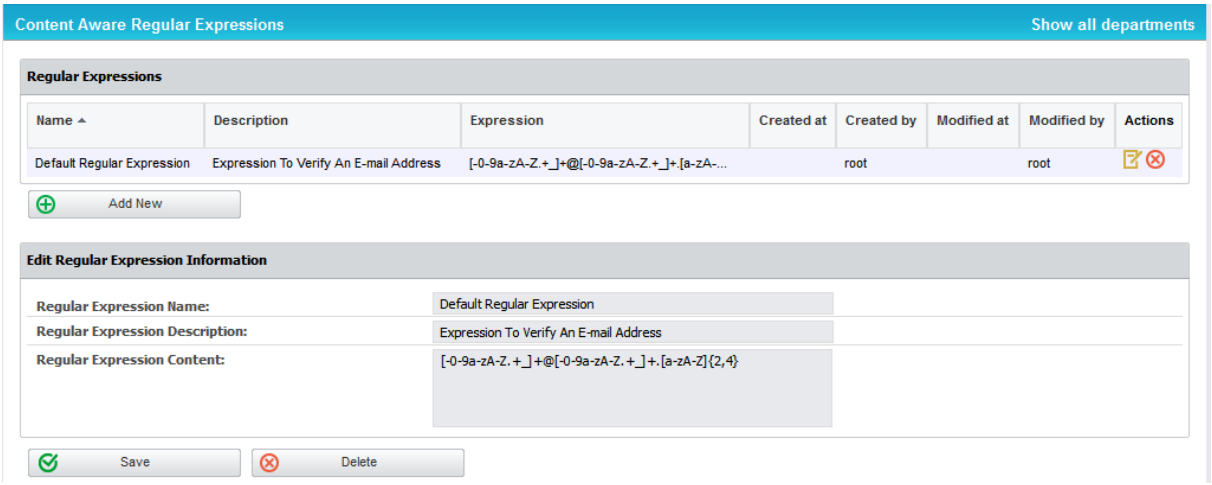
Domain Whitelists are custom defined e-mail addresses to which sending of confidential information will be allowed by the Endpoint Protector .This feature works on Microsoft Outlook and Mozilla Thunderbird.



Once a new domain whitelist is added, it will be automatically displayed inside the Domain Whitelists tab.

7.6. Content Aware Regex (Regular Expressions)

By definition, Regular Expressions are sequences of characters that form a search pattern, mainly for use in pattern matching with strings. An administrator can create a regular expression in order to find a certain recurrence in the data that is transferred across the protected network.



Example that matches an e-mail: **[-0-9a-zA-Z.+_]+@[-0-9a-zA-Z.+_]+\.[a-zA-Z]{2,4}**

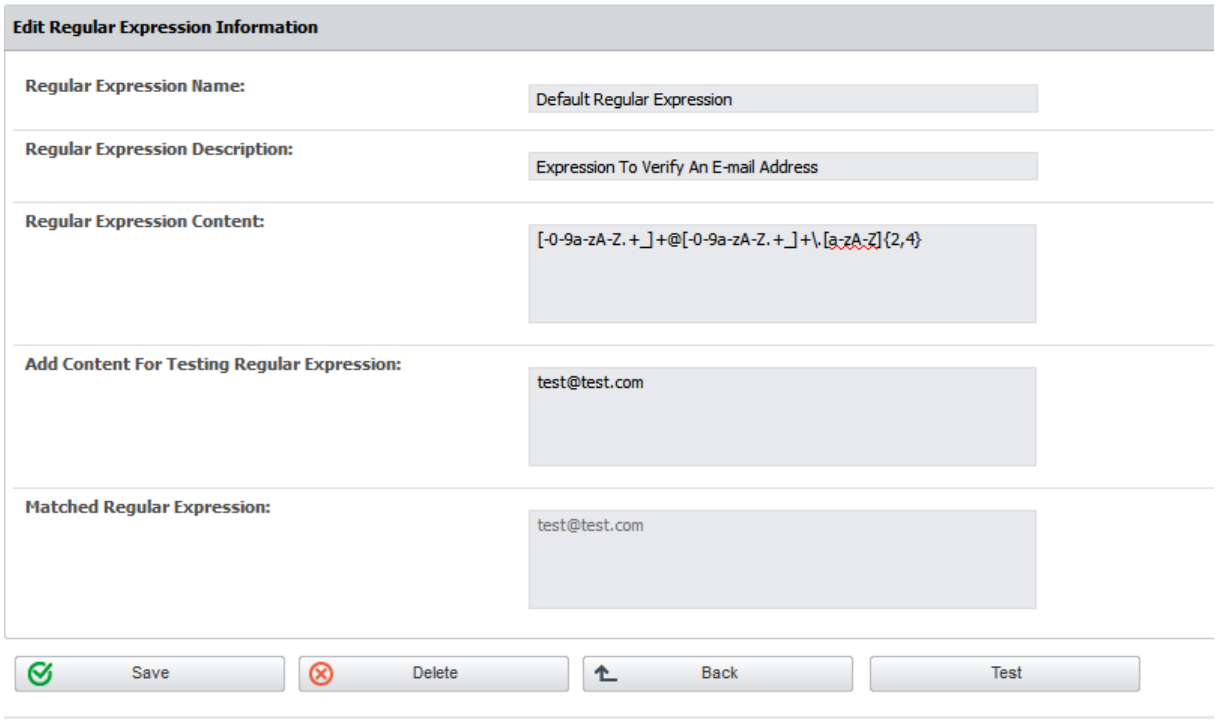
Example that matches an IP: **(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)(\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)){3}**

Note!

If possible, avoid using Regular Expressions, as their complexity typically increases the resources usage. Using a large number of regular expressions as filtering criteria typically increases CPU usage. Also, improper regular expressions or improper use can have negative implications.

This feature is provided "as is" and requires advanced knowledge of the Regular Expression syntax.
The regular expressions feature is provided with no direct support and it is the responsibility of the customers to learn and implement regular expressions and to thoroughly test.

Regular Expressions can be tested for accuracy. Insert into the "Add Content for Testing Regular Expression" box a general example of something on which the regex applies to, and press the "Test" button. If the Regular Expression has no errors inside of it, then the same content should appear into the "Matched Regular Expression" box, as shown below:



7.7. How Content Aware Protection works for monitored Applications / Online Services

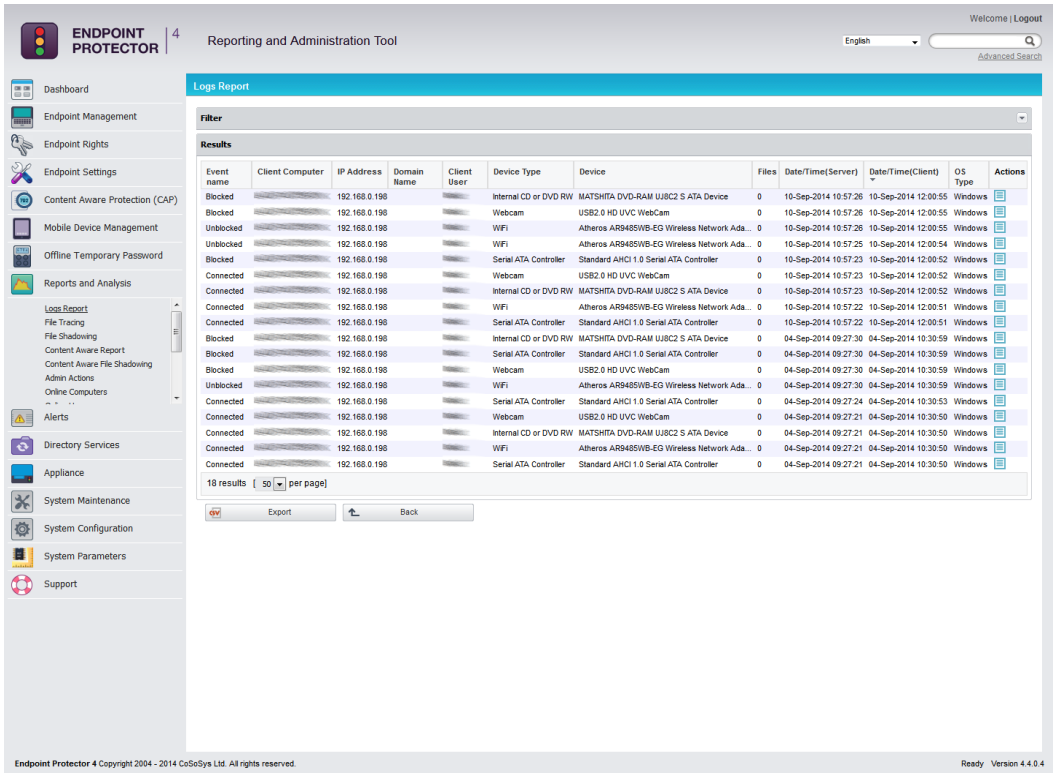
The following table shows a list of actions and content that are screened/inspected or left unscreened/uninspected by the Content Aware Protection feature.

APPLICATION	SCREENED	NOT SCREENED
Web Browsers	Uploaded Files Webmail Attachments	Webpage Content Downloaded Content Blog Posts
E-MAIL Clients	File Attachments Microsoft Outlook E-MAIL Content Microsoft Outlook Forwarded and Saved Attachments Microsoft Outlook E-mailed directly from Windows Explorer Microsoft Outlook Copied Attachments from one E-MAIL to another Mozilla Thunderbird E-MAIL Content	E-MAIL Content for other E-MAIL Services Forwarded Attachments Saved Attachments Attachments e-mailed directly from Windows Explorer Copied Attachments from one E-MAIL to another
Instant Messaging	File Transfers Shared Picture Files	IM Message Content Sent Files
File Sharing	File Uploads	Saved Files
Social Media/Other	File Transfers	Blog Posts

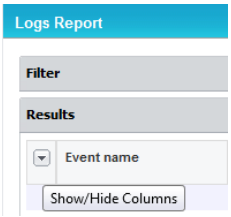
*Other limitations may apply.

8. Reports and Analysis

This module is designed to offer the administrator feedback regarding system functionality and information related to devices, users and computers in the entire system.



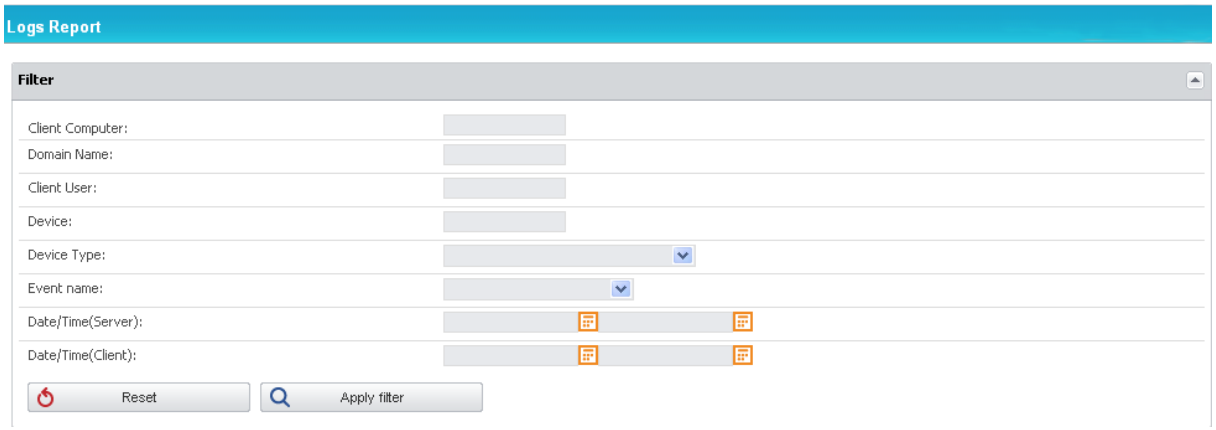
All tabs described below will have a filter option at the beginning of each table. This will add or remove columns based on the content considered relevant.



8.1. Logs Report

The most powerful and detailed representation of activity recordings can be achieved using this module. It allows the administrator to see exactly what actions took place at what time. This information also contains the computer name, user and device used and also the action taken and the files accessed.

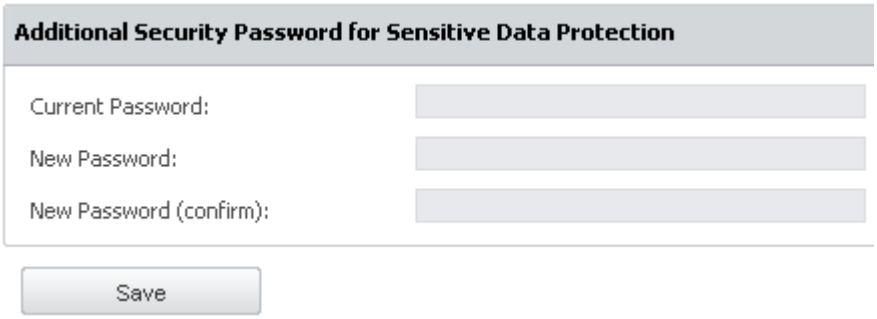
The granular filter included in this module is designed to make finding information quick and easy.



The administrator has the possibility of exporting either the search results or the entire log report as a .CSV file, which can later be printed out for detailed analysis.

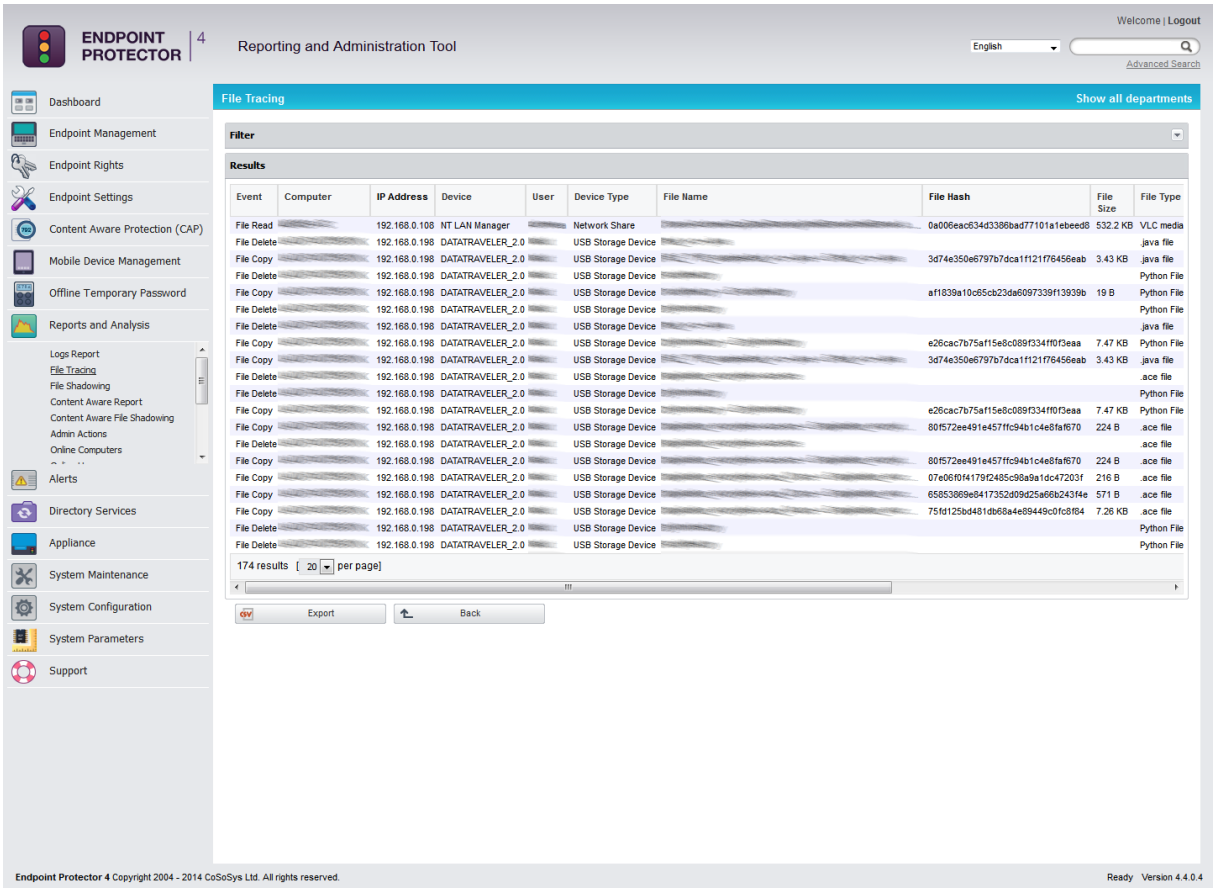
As an additional data security measure, this module may be protected by an additional password set by the Super Administrator.

The additional security password can be set from the System Configuration module, under the System Security tab and it applies to all the Reports and Analysis sections.



8.2. File Tracing

Displays the list of file properties traced of files that have been transferred from a protected computer to a portable device or another computer on the network, and vice versa. It also displays the original location of the transferred files if Detect Source Copy is activated from System Policies or Global Settings.



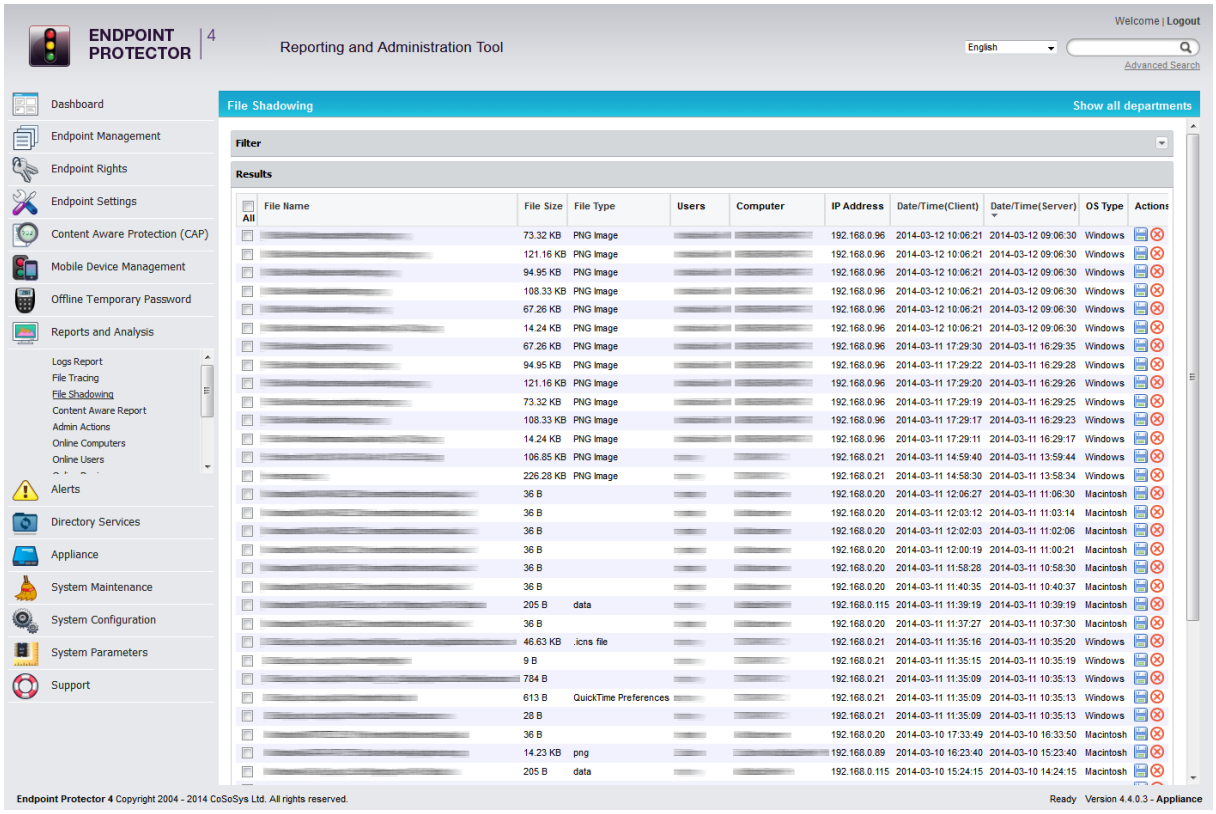
Similar with the Logs Reports section, you may need to enter an additional password set by the administrator in order to be able to access the list of files.

A special mention is given here to the “File Hash” column. The Endpoint Protector application computes an MD5 hash for most of the files on which the File Tracing feature applies to. By this way we ensure that threats coming from the changing of the content inside of files is mitigated.

8.3. File Shadowing

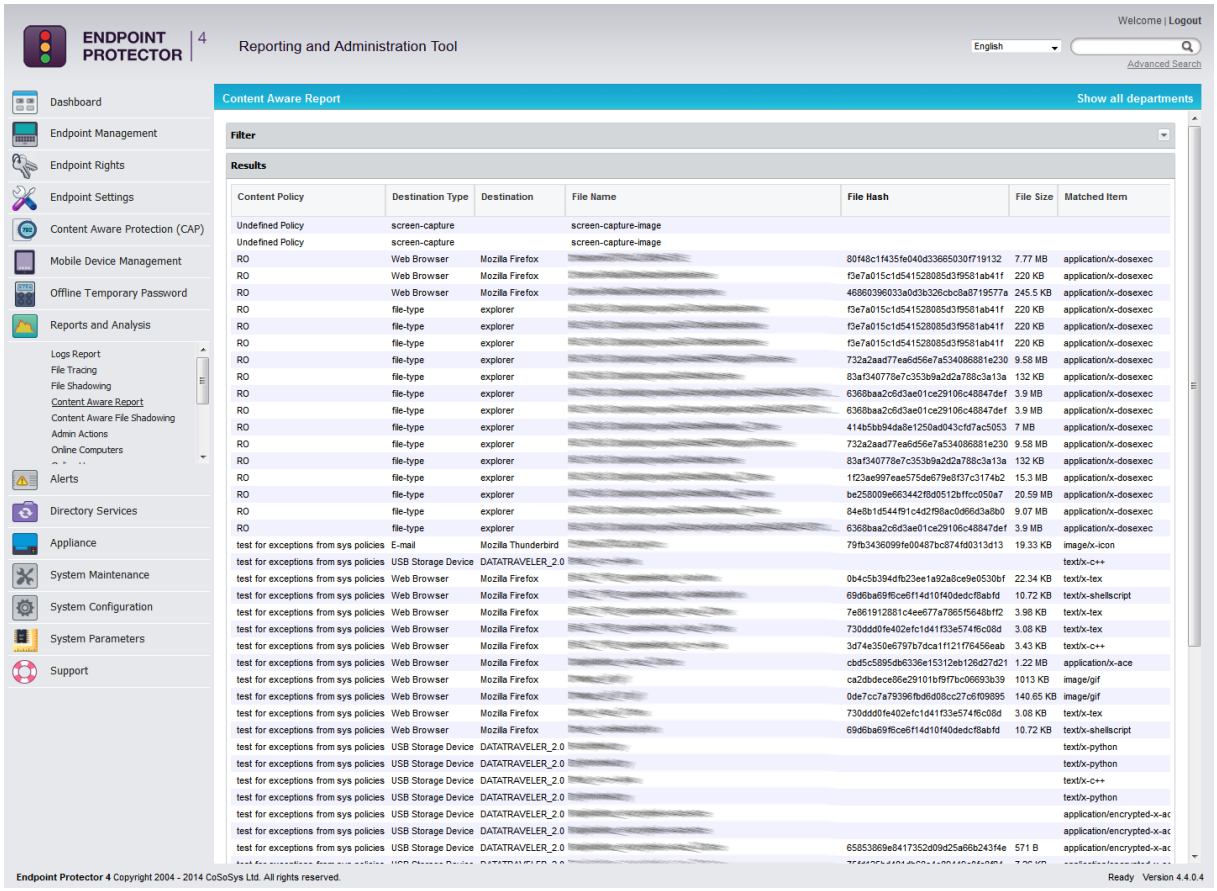
Displays the list of file shadows and files that have been transferred from a protected computer to a portable device. The list of files may be protected by an additional password set by the administrator. In this case, you will be prompted to insert the additional password when entering this section.

Additionally, the shadowed files can be saved locally on the Server by the Endpoint Protector administrator.



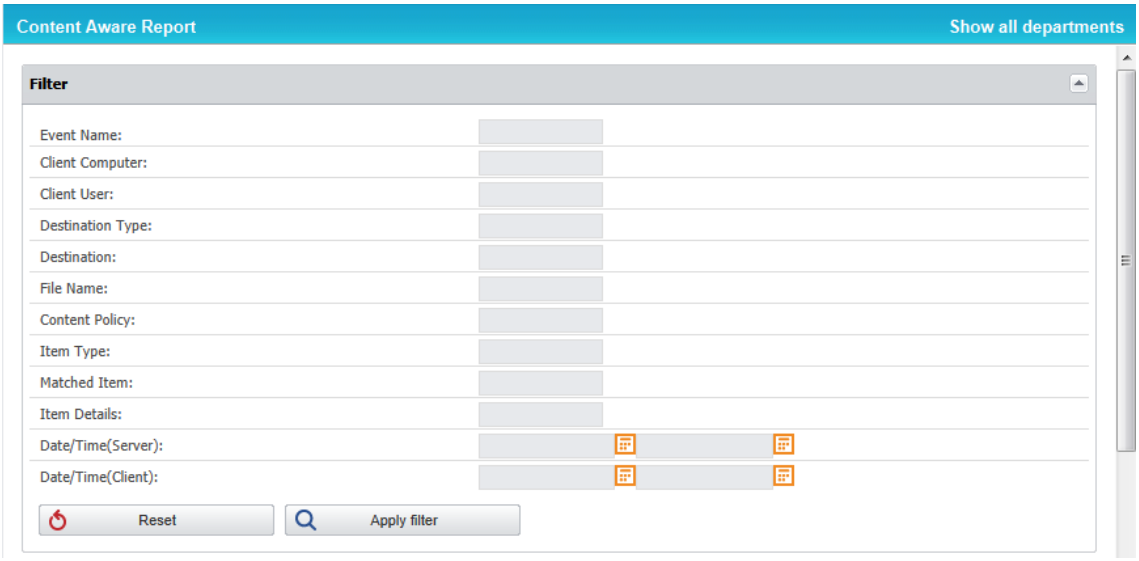
8.4. Content Aware Report

This module provides detailed logs of all Content Aware activity. It allows the administrator to see exactly what data incidents were detected corresponding to the Content Aware Policies applied and at what time. This information also contains the computer name, user and transfer destination type, the action taken and the file inspected. The included granular filter is designed to make finding information quick and easy.



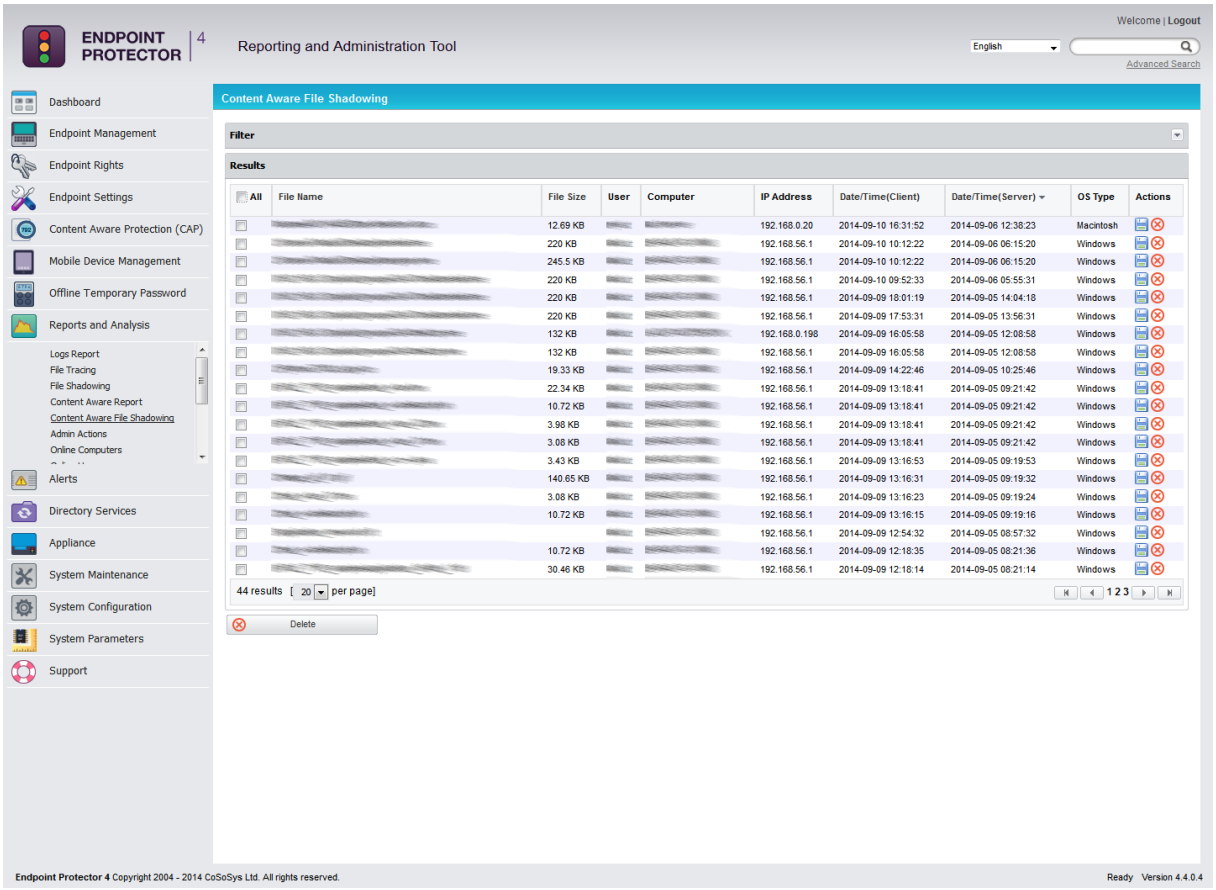
The administrator has the possibility of exporting both the search results and the entire log report as a .CSV file, which can later be printed out for detailed auditing.

As an additional data security measure, this module may be protected by an additional password set by the Super Administrator. For more details, please see section 8.1. Logs Report.



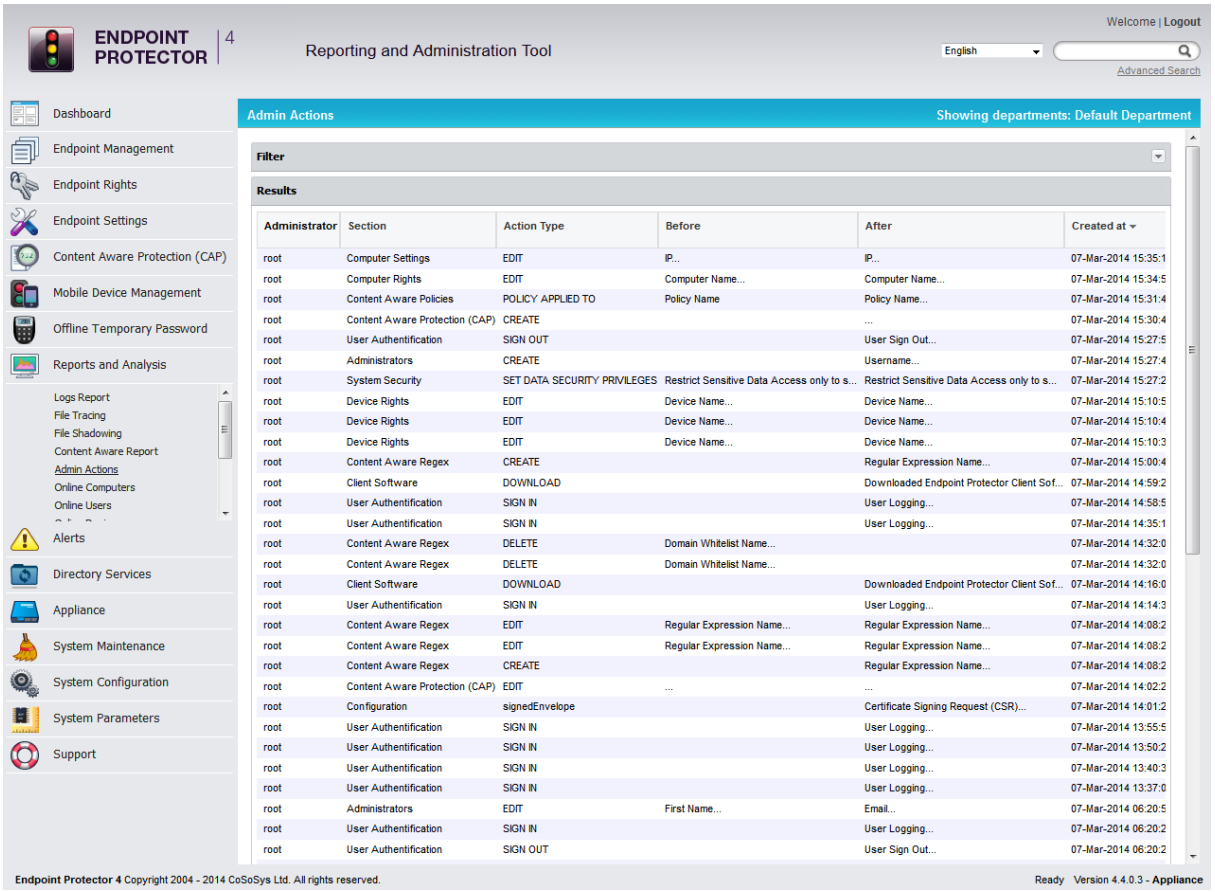
8.5. Content Aware File Shadowing

Displays the list of file shadows and files that have been detected by a Content Aware policy. The list of files may be protected by the additional password set by the administrator for all the Reports and Analysis sections. In this case, you will be prompted to insert the additional password when entering this section.



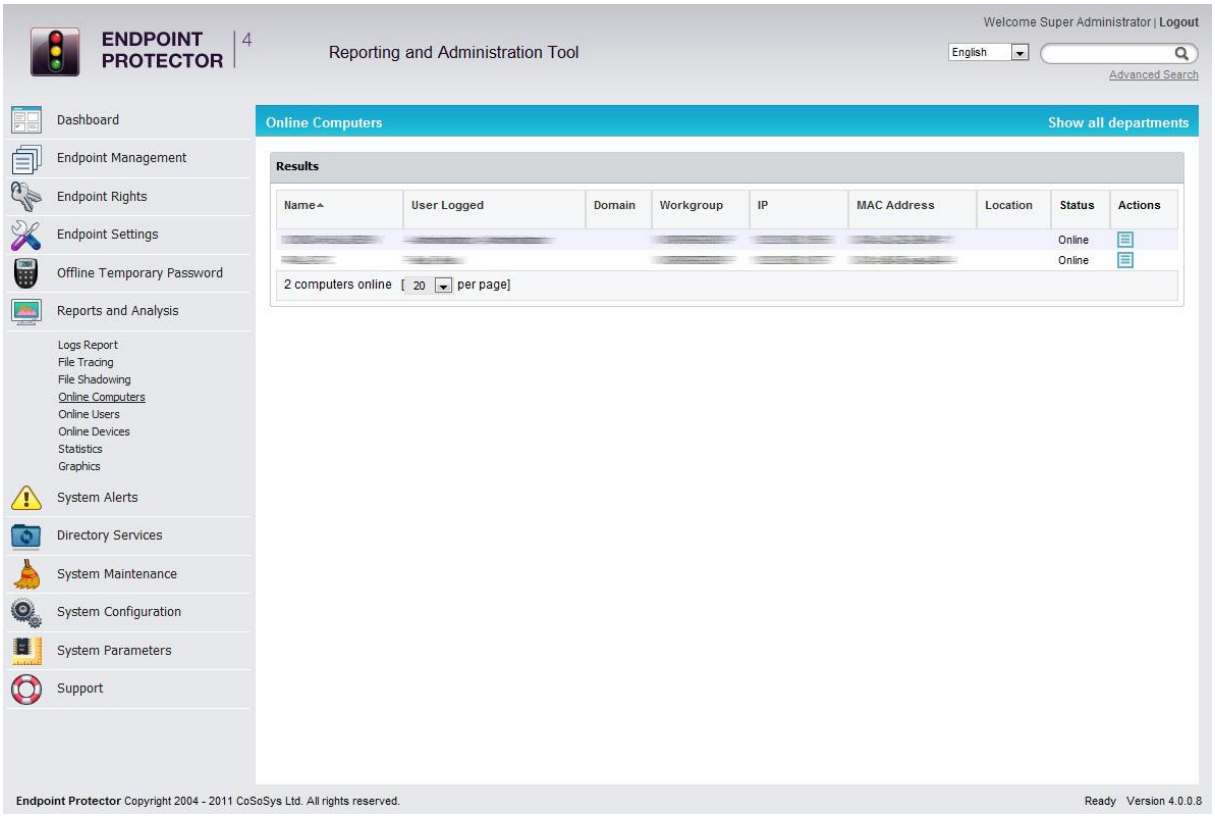
8.6. Admin Actions

Every important action performed by administrators in the interface is recorded. Clicking the "view details" button will open the "Admin Actions Details" page where further details about the specific event is shown, with the status of the modified feature before and after the change took place.


ENDPOINT PROTECTOR 4
Reporting and Administration Tool
Welcome | Logout
English
Advanced Search
Dashboard
Endpoint Management
Endpoint Rights
Endpoint Settings
Content Aware Protection (CAP)
Mobile Device Management
Offline Temporary Password
Reports and Analysis
Logs Report
File Tracing
File Shadowing
Content Aware Report
Admin Actions
Online Computers
Online Users
Alerts
Directory Services
Appliance
System Maintenance
System Configuration
System Parameters
Support
Admin Actions
Showing departments: Default Department
Filter
Results
Administrator | Section | Action Type | Before | After | Created at
root | Computer Settings | EDIT | IP... | IP... | 07-Mar-2014 15:35:1
root | Computer Rights | EDIT | Computer Name... | Computer Name... | 07-Mar-2014 15:34:5
root | Content Aware Policies | POLICY APPLIED TO | Policy Name | Policy Name... | 07-Mar-2014 15:31:4
root | Content Aware Protection (CAP) | CREATE | | ... | 07-Mar-2014 15:30:4
root | User Authentification | SIGN OUT | | User Sign Out... | 07-Mar-2014 15:27:5
root | Administrators | CREATE | | Username... | 07-Mar-2014 15:27:4
root | System Security | SET DATA SECURITY PRIVILEGES | Restrict Sensitive Data Access only to s... | Restrict Sensitive Data Access only to s... | 07-Mar-2014 15:27:2
root | Device Rights | EDIT | Device Name... | Device Name... | 07-Mar-2014 15:10:5
root | Device Rights | EDIT | Device Name... | Device Name... | 07-Mar-2014 15:10:4
root | Device Rights | EDIT | Device Name... | Device Name... | 07-Mar-2014 15:10:3
root | Content Aware Regex | CREATE | | Regular Expression Name... | 07-Mar-2014 15:00:4
root | Client Software | DOWNLOAD | | Downloaded Endpoint Protector Client Sof... | 07-Mar-2014 14:59:2
root | User Authentification | SIGN IN | | User Logging... | 07-Mar-2014 14:58:5
root | User Authentification | SIGN IN | | User Logging... | 07-Mar-2014 14:35:1
root | Content Aware Regex | DELETE | Domain Whitelist Name... | | 07-Mar-2014 14:32:0
root | Content Aware Regex | DELETE | Domain Whitelist Name... | | 07-Mar-2014 14:32:0
root | Client Software | DOWNLOAD | | Downloaded Endpoint Protector Client Sof... | 07-Mar-2014 14:16:0
root | User Authentification | SIGN IN | | User Logging... | 07-Mar-2014 14:14:3
root | Content Aware Regex | EDIT | Regular Expression Name... | Regular Expression Name... | 07-Mar-2014 14:08:2
root | Content Aware Regex | EDIT | Regular Expression Name... | Regular Expression Name... | 07-Mar-2014 14:08:2
root | Content Aware Regex | CREATE | | Regular Expression Name... | 07-Mar-2014 14:08:2
root | Content Aware Protection (CAP) | EDIT | ... | ... | 07-Mar-2014 14:02:2
root | Configuration | signedEnvelope | | Certificate Signing Request (CSR)... | 07-Mar-2014 14:01:2
root | User Authentification | SIGN IN | | User Logging... | 07-Mar-2014 13:55:5
root | User Authentification | SIGN IN | | User Logging... | 07-Mar-2014 13:50:2
root | User Authentification | SIGN IN | | User Logging... | 07-Mar-2014 13:40:3
root | User Authentification | SIGN IN | | User Logging... | 07-Mar-2014 13:37:0
root | Administrators | EDIT | First Name... | Email... | 07-Mar-2014 06:20:5
root | User Authentification | SIGN IN | | User Logging... | 07-Mar-2014 06:20:2
root | User Authentification | SIGN OUT | | User Sign Out... | 07-Mar-2014 06:20:2
Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.
Ready Version 4.4.0.3 - Appliance

The logs can be exported in a .csv file, while the filter can help find the desired information quickly and easily.

8.7. Online Computers



Offers real time* monitoring of the client computers registered on the system which have an established connection with the server.

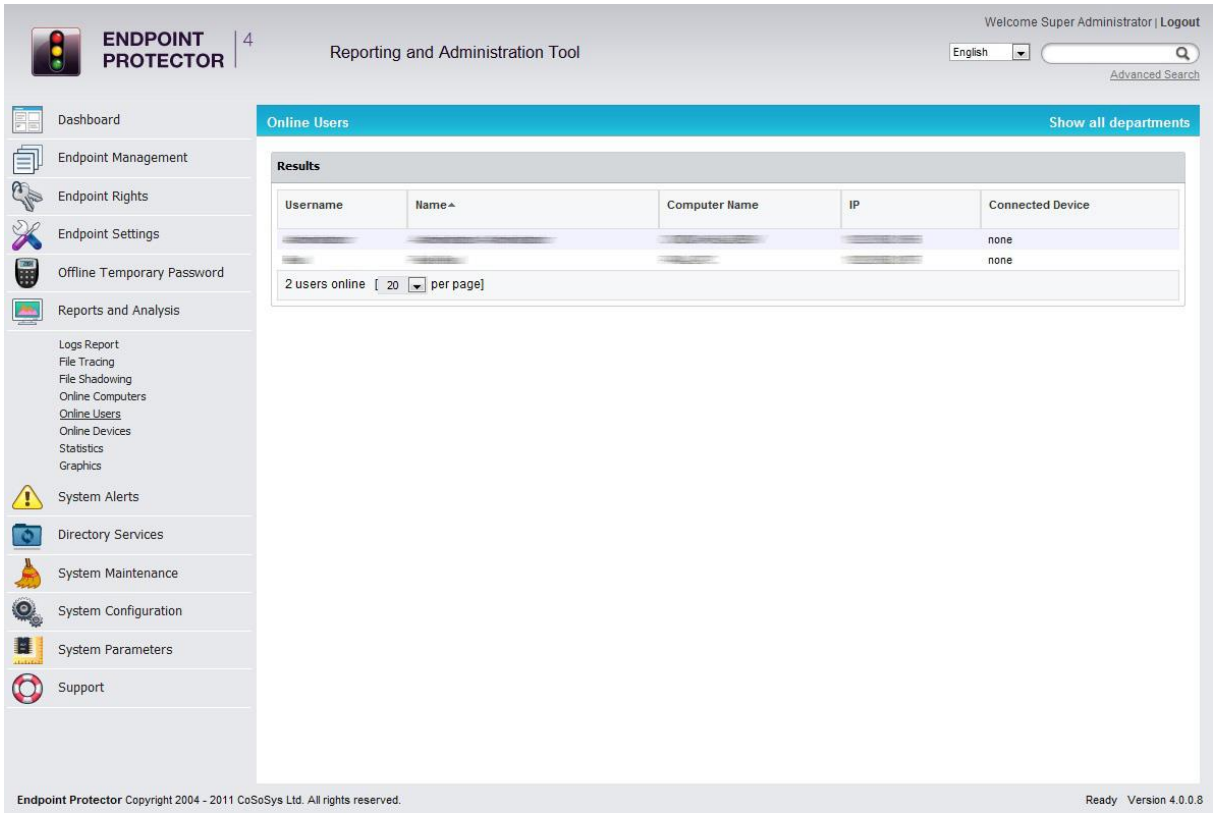
*depends on the Refresh Interval; if the Refresh Interval for computer X is 1 minute, than the computer X was communicating with the server in the last 1 minute.

The administrator has the possibility of accessing the log for a certain computer by pressing the “View Logs” action button.

Pressing this button will take you to the logs report where it will only display the actions of that specific computer for which the button was pushed.

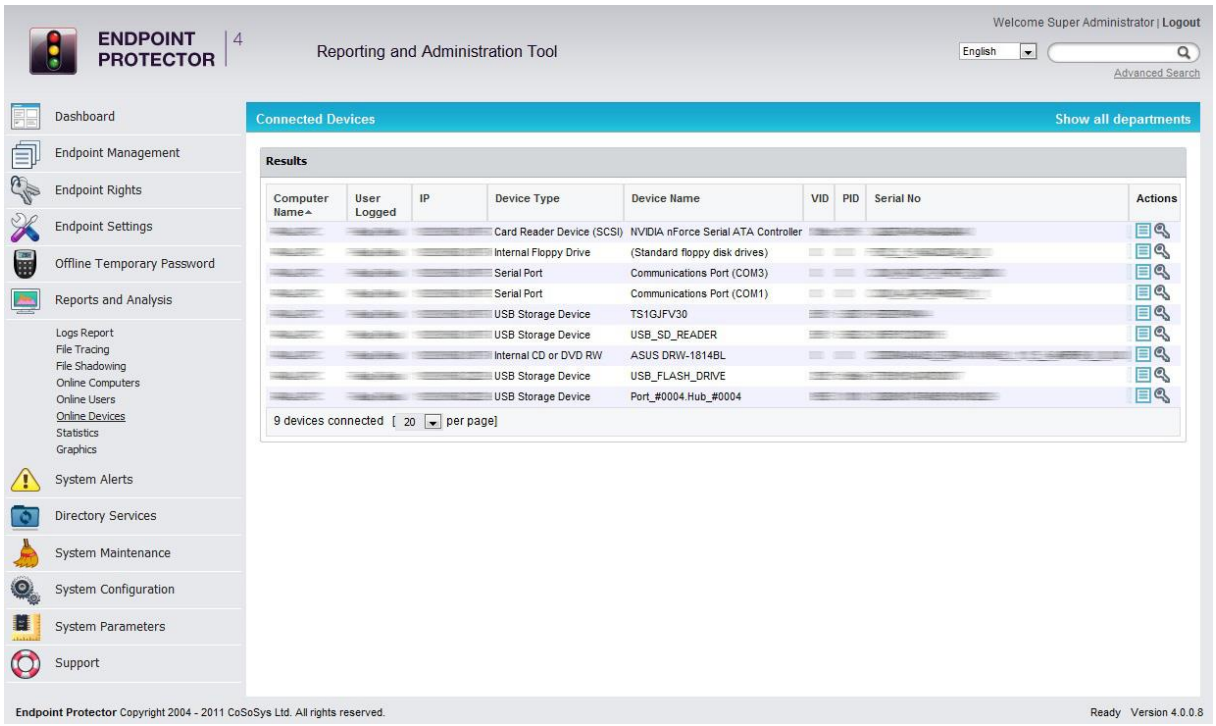
8.8. Online Users

Shows a list of users that are connected to the Endpoint Protector Server in real time.


ENDPOINT PROTECTOR 4
Reporting and Administration Tool
Welcome Super Administrator | Logout
English
Advanced Search
Dashboard
Endpoint Management
Endpoint Rights
Endpoint Settings
Offline Temporary Password
Reports and Analysis
Logs Report
File Tracing
File Shadowing
Online Computers
Online Users
Online Devices
Statistics
Graphics
System Alerts
Directory Services
System Maintenance
System Configuration
System Parameters
Support
Online Users
Show all departments
Results
Username
Name
Computer Name
IP
Connected Device
none
none
2 users online [20 per page]
Endpoint Protector Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved.
Ready Version 4.0.0.8

8.9. Online Devices

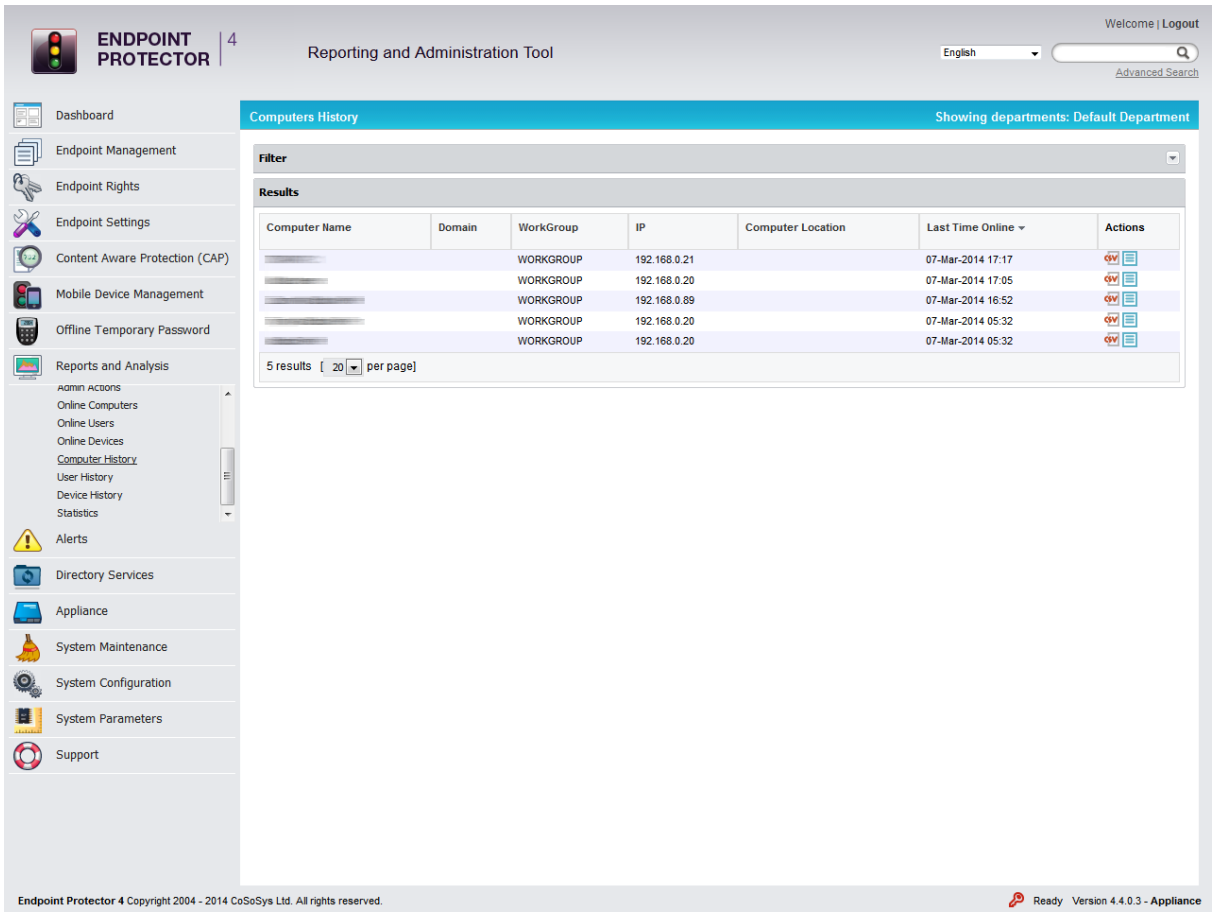
Offers information regarding the devices connected to the computers on the system.



The administrator can see which devices are connected to what computers and also the client user who is accessing them. The administrator can also use the action buttons “View Logs” and “Manage Rights” to quickly administer the device.

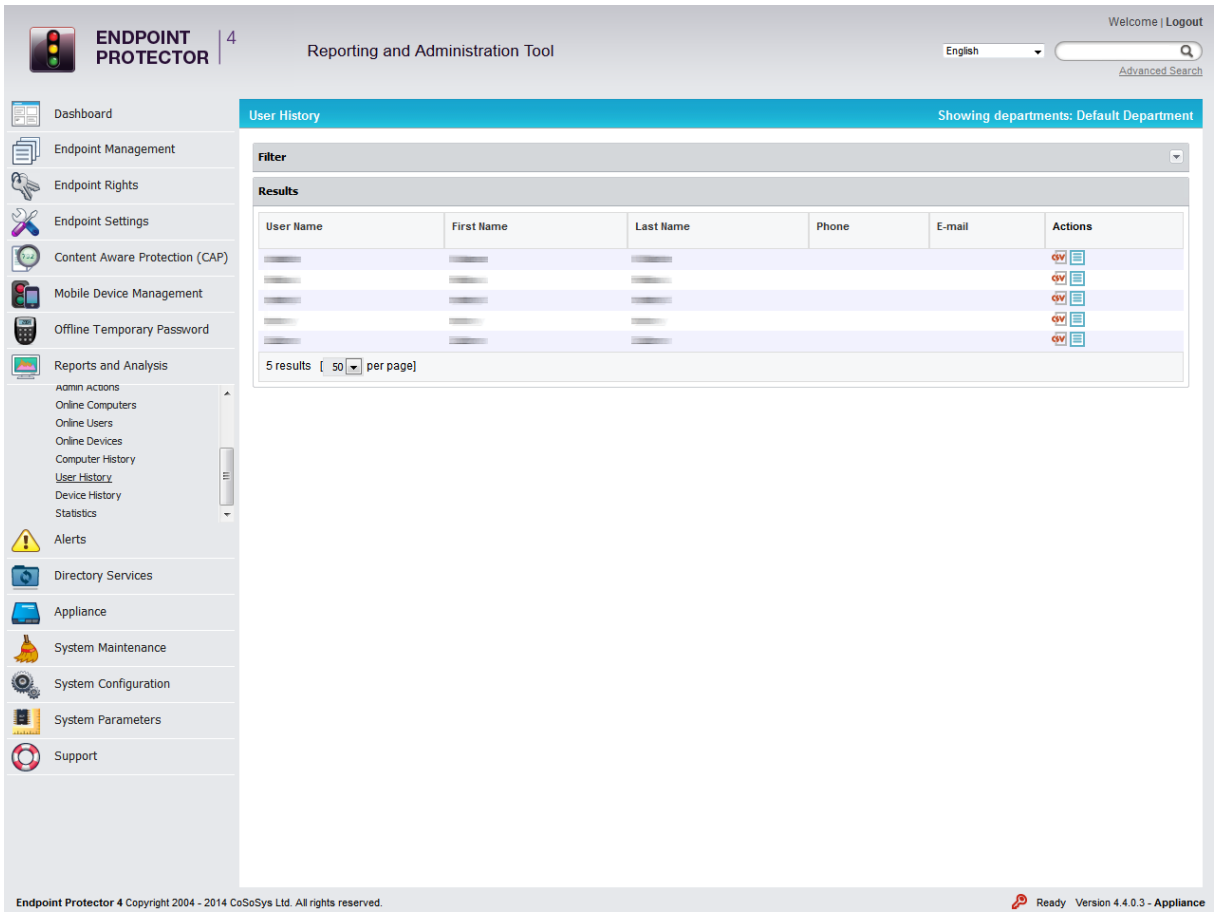
8.10. Computer History

This module shows all computers that were at least once connected to the server. With the help of the “Export” button the logs can be saved to a .csv file, while pressing the “View Machine log” will show the Logs Report page filtered for the respective Computer.



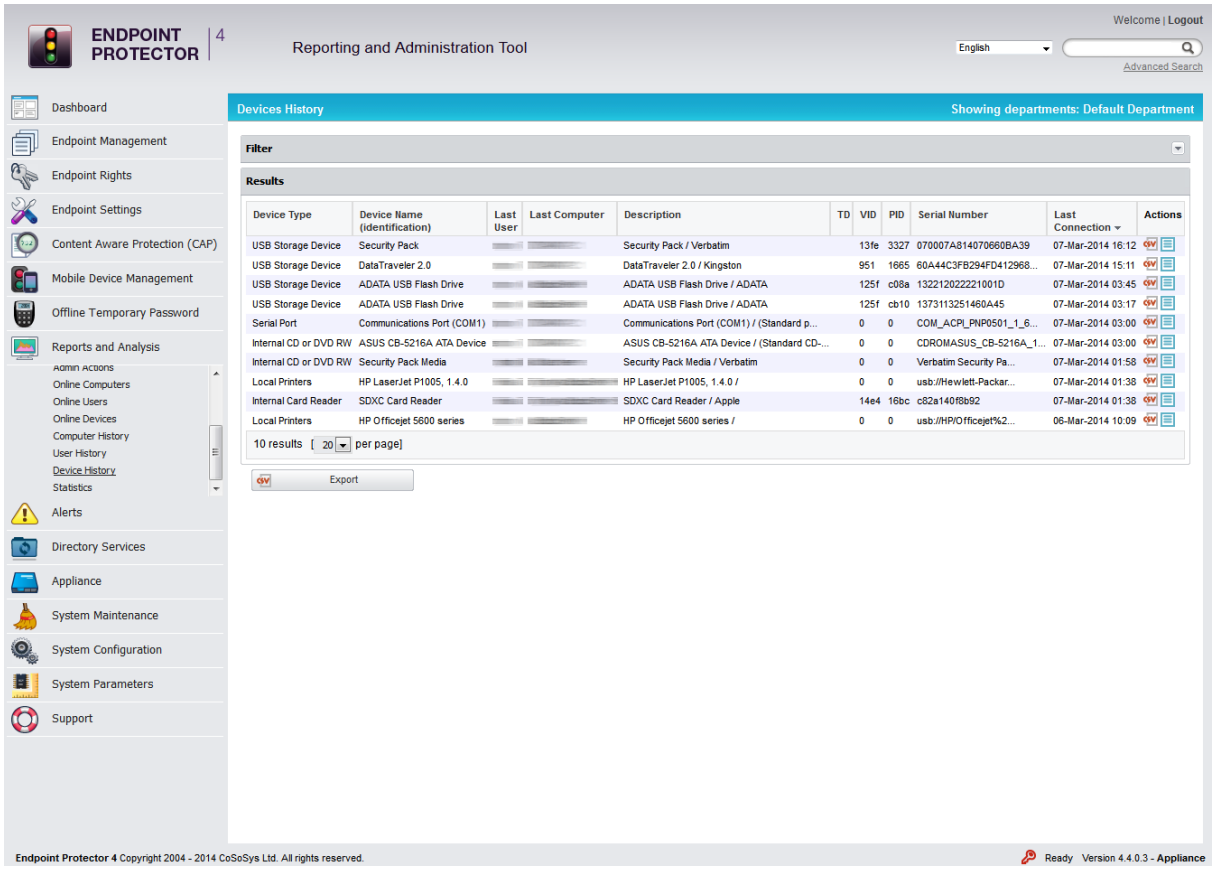
8.11. User History

This module shows all users that were at least once connected to the server. With the help of the "Export" button the logs can be saved to a .csv file, while pressing the "View User log" will show the Logs Report page filtered for the respective User.



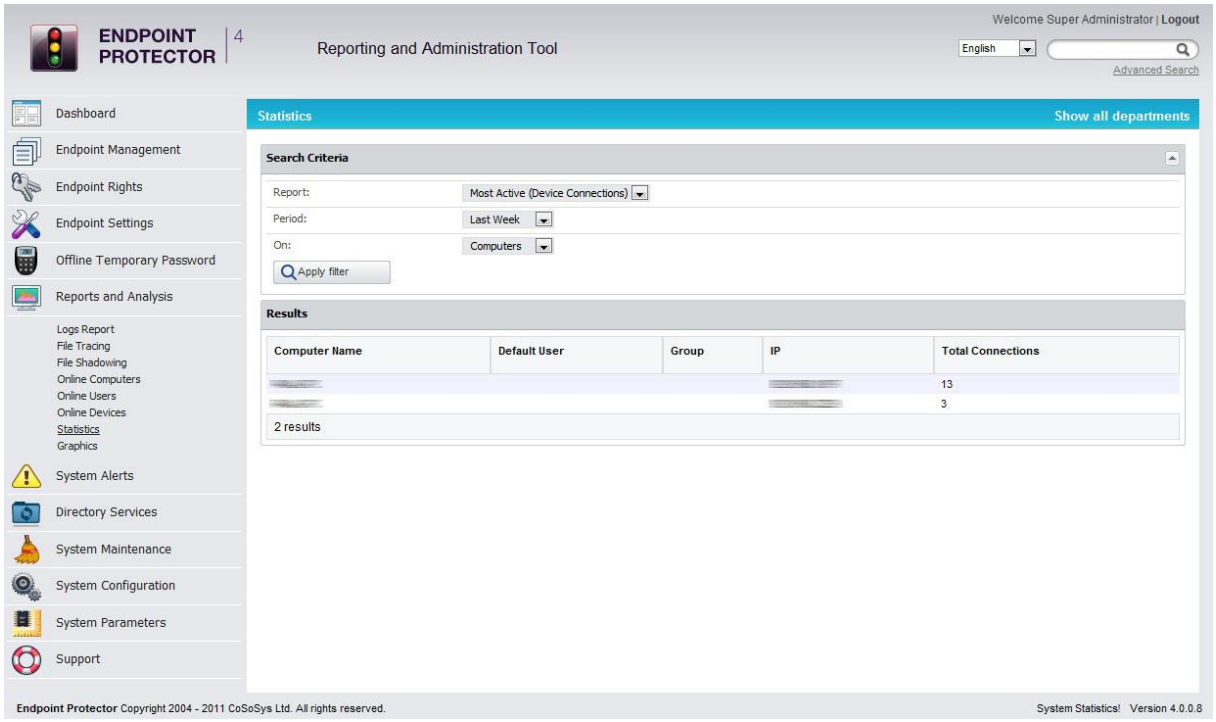
8.12. Device History

Similar to Computer and User history, all devices that were at least once connected to the server can be found here. Logs can be exported to a .csv file by pressing the “Export” button, while “View Device Log” will show the Logs Report page filtered for the respective device.


ENDPOINT PROTECTOR 4
Reporting and Administration Tool
Welcome | Logout
English
Advanced Search
Dashboard
Endpoint Management
Endpoint Rights
Endpoint Settings
Content Aware Protection (CAP)
Mobile Device Management
Offline Temporary Password
Reports and Analysis
Admin Actions
Online Computers
Online Users
Online Devices
Computer History
User History
Device History
Statistics
Alerts
Directory Services
Appliance
System Maintenance
System Configuration
System Parameters
Support
Devices History
Showing departments: Default Department
Filter
Results
Device Type
Device Name (identification)
Last User
Last Computer
Description
TD
VID
PID
Serial Number
Last Connection
Actions
USB Storage Device Security Pack Security Pack / Verbatim 13fe 3327 070007A814070660BA39 07-Mar-2014 16:12
USB Storage Device DataTraveler 2.0 DataTraveler 2.0 / Kingston 951 1665 60A44C3FB294FD412968... 07-Mar-2014 15:11
USB Storage Device ADATA USB Flash Drive ADATA USB Flash Drive / ADATA 125f c08a 1322120222221001D 07-Mar-2014 03:45
USB Storage Device ADATA USB Flash Drive ADATA USB Flash Drive / ADATA 125f cb10 1373113251460A45 07-Mar-2014 03:17
Serial Port Communications Port (COM1) Communications Port (COM1) / (Standard p... 0 0 COM_ACPI_PNP0501_1_6... 07-Mar-2014 03:00
Internal CD or DVD RW ASUS CB-5216A ATA Device ASUS CB-5216A ATA Device / (Standard CD-... 0 0 CDROM\ASUS_CB-5216A_1... 07-Mar-2014 03:00
Internal CD or DVD RW Security Pack Media Security Pack Media / Verbatim 0 0 Verbatim Security Pa... 07-Mar-2014 01:58
Local Printers HP LaserJet P1005, 1.4.0 HP LaserJet P1005, 1.4.0 / 0 0 usb://Hewlett-Packar... 07-Mar-2014 01:38
Internal Card Reader SDXC Card Reader SDXC Card Reader / Apple 14e4 16bc c82a140f8b92 07-Mar-2014 01:38
Local Printers HP Officejet 5600 series HP Officejet 5600 series / 0 0 usb://HP/Officejet%2... 06-Mar-2014 10:09
10 results [20 per page]
Export
Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.
Ready Version 4.4.0.3 - Appliance

8.13. Statistics

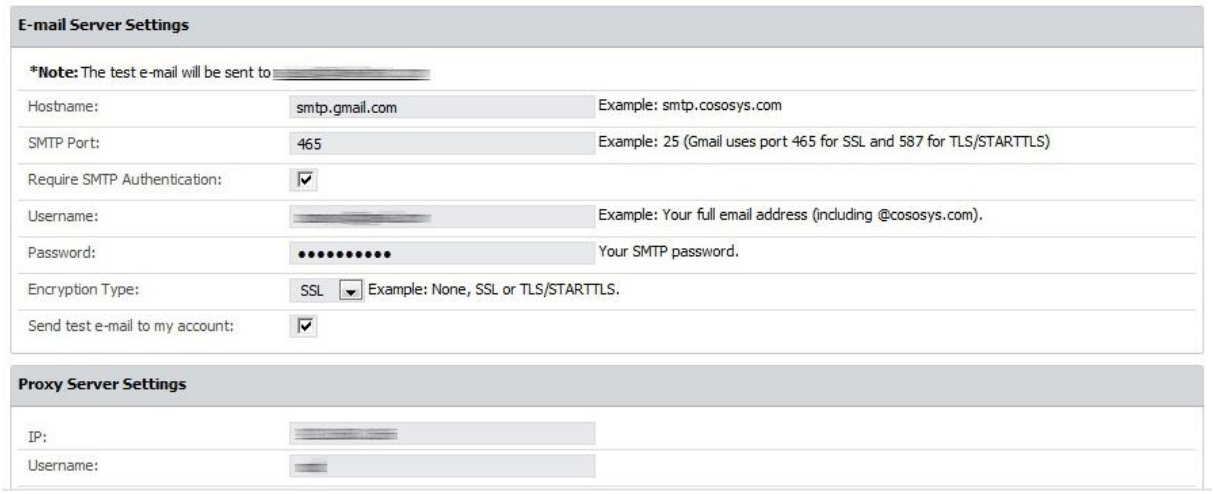
The Statistics module will allow you to view system activity regarding data traffic and device connections. The integrated filter makes generating reports easy and fast. Simply select the field of interest and click the “Apply filter” button.



9. Alerts

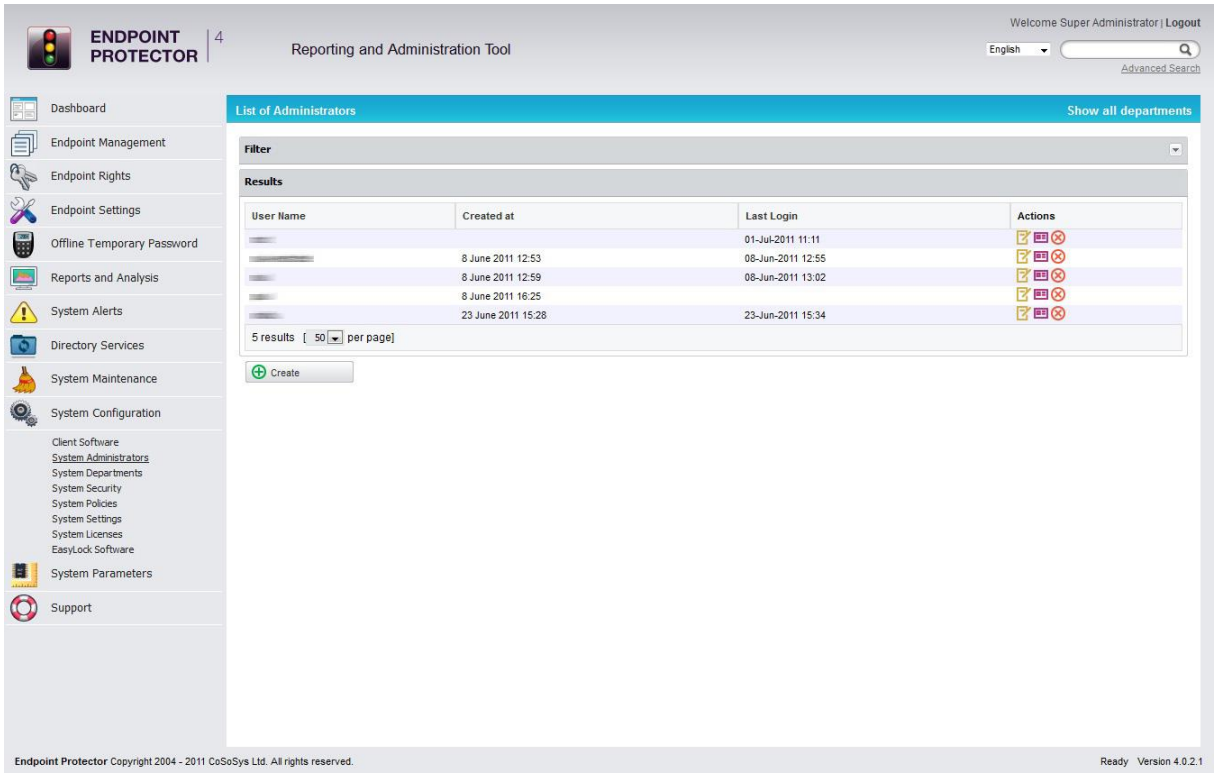
Endpoint Protector allows you to set notifications (Alerts) for Sensitive Content Transfers, Devices, Computers, Groups and Users making monitoring them easier. An Alert will trigger an E-MAIL that will be sent to the selected administrator(s) that are intended to receive the alerts. You can set up device related activity alerts in the System Alerts-> Define System Alerts module in Endpoint Protector. The Define Content Aware Alerts option will allow administrators to set special alerts for sensitive content detection and transfer blocking.

Before you can create an E-MAIL alert, you must configure the server host and provide a user name and password to that mail server. You can do that by accessing "System Settings" in the "System Configuration" module.



You can also verify if your settings are correct by checking the box next to "Send test E-MAIL to my account".

You also have to configure the E-MAIL of your current user with which you are accessing Endpoint Protector; by default, "root". To do this, go to "System Configuration" > "System Administrators".

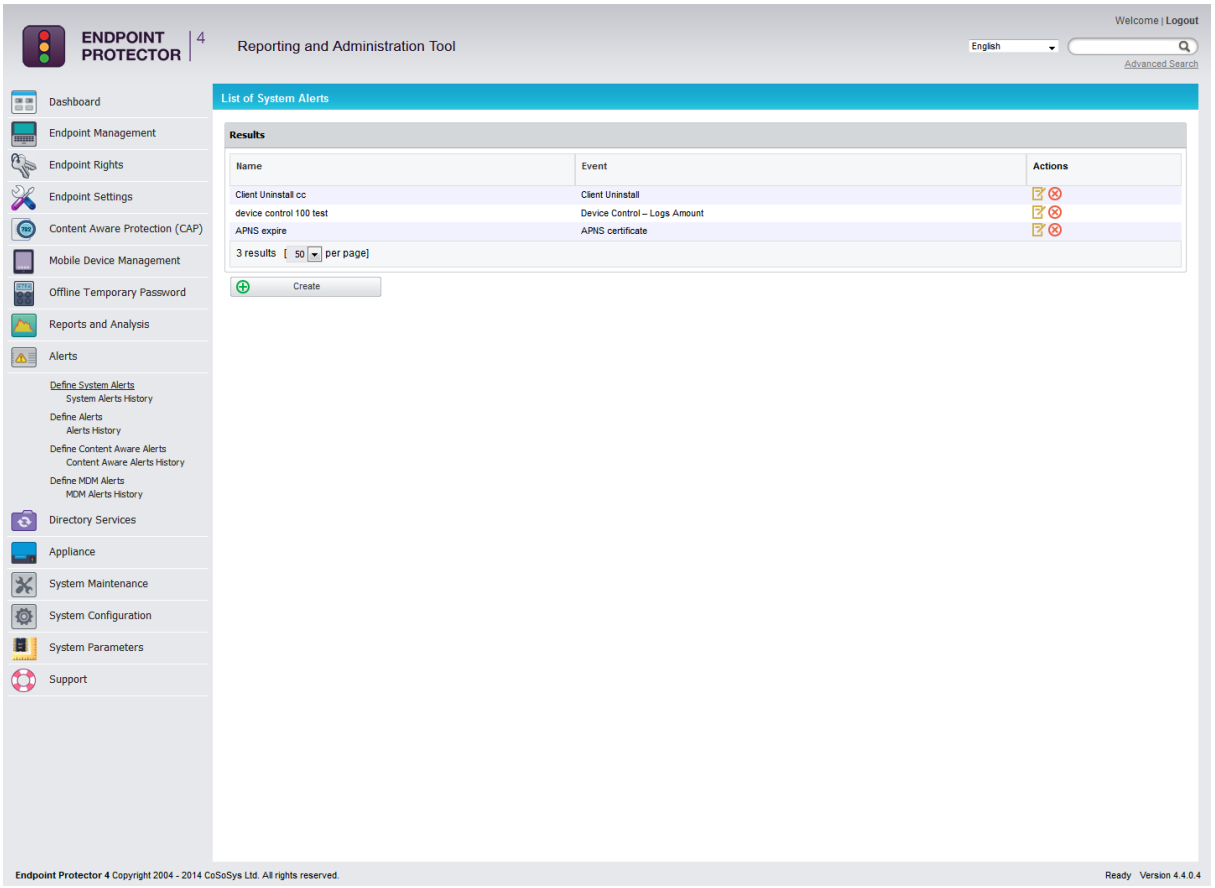


The actions available here are Edit, Edit Info and Delete.

Select the option “Edit info” for the desired user and complete the required fields. After you are done, click “Save”.

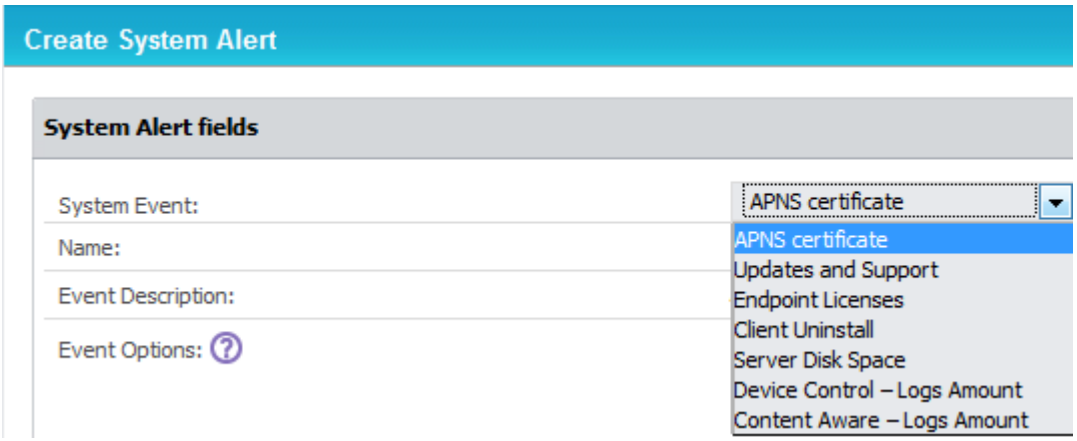
Now you are set up to receive E-MAIL alerts.

9.1. Define System Alerts



To create a new system alert, go to "Define System Alerts" and click "Create".

There are several types of alerts available as shown below:



APNS certificate – APNS certificates expire and have to be renewed on a regular basis. These alerts eliminates the risks of having to re-enroll all the mobile devices by sending an e-mail reminder 60, 30 or 10 days prior.

Updates and Support – To ensure the Endpoint Protector Appliance is up to date, a reminder can be sent regarding each module maintenance status (Device Control, Content Aware Protection and Mobile Device Management).

Endpoint Licenses – As each network is constantly growing, to eliminate the risks of having unprotected endpoints, an alert can be generated. It can be defined if the percentage of already used Endpoint Licenses reaches 70%, 80% or 90%.

Client Uninstall – For a better management of a large network, an alert can be sent each time an Endpoint Protector Client is uninstalled. This is particularly helpful when there are several assigned Administrators.

Server Disk Space – Ensuring Server Disk Space remains available for logs to be stored and policies are properly applied, and alert can be setup when disk space reaches 70%, 80% or 90%.

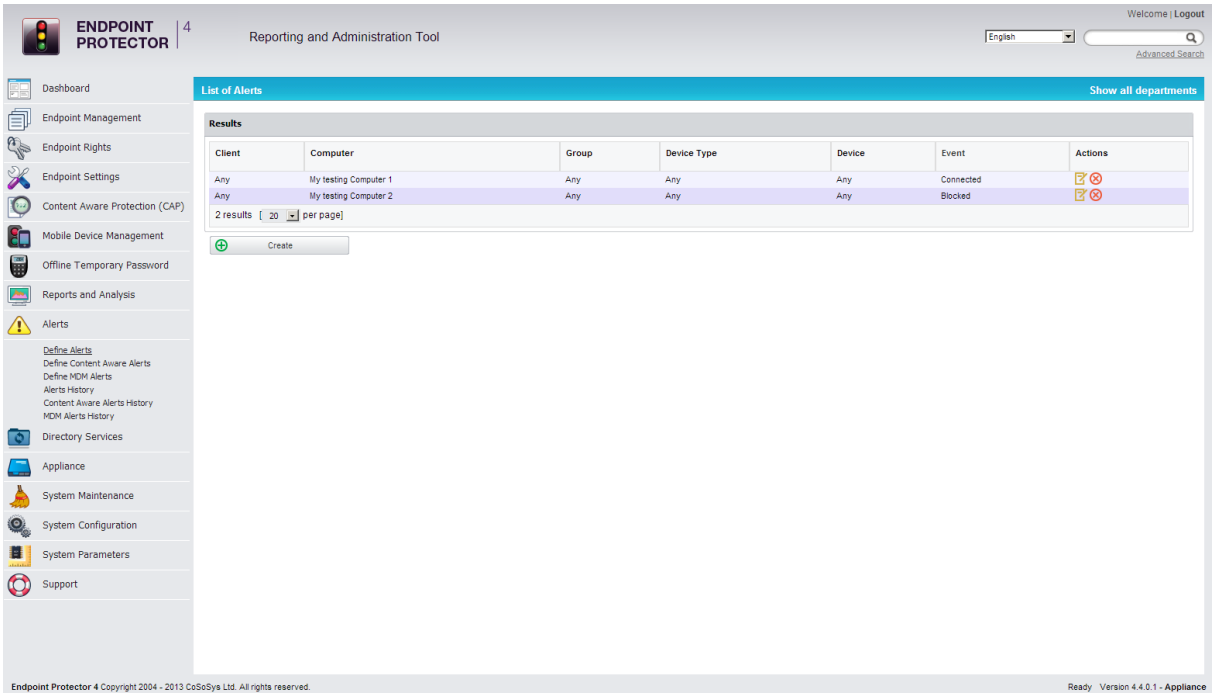
Device Control – Logs Amount – An alert can be sent each time the Number of Device Control Logs Stored reaches a specific amount. The option to choose either from an interval between 10,000 rows or 10,000,000 rows or define a desired value are available.

Content Aware – Logs Amount – An alert can be sent each time the Number of Content Aware Logs Stored reaches a specific amount. The option to choose either from an interval between 10,000 rows or 10,000,000 rows or define a desired value are available.

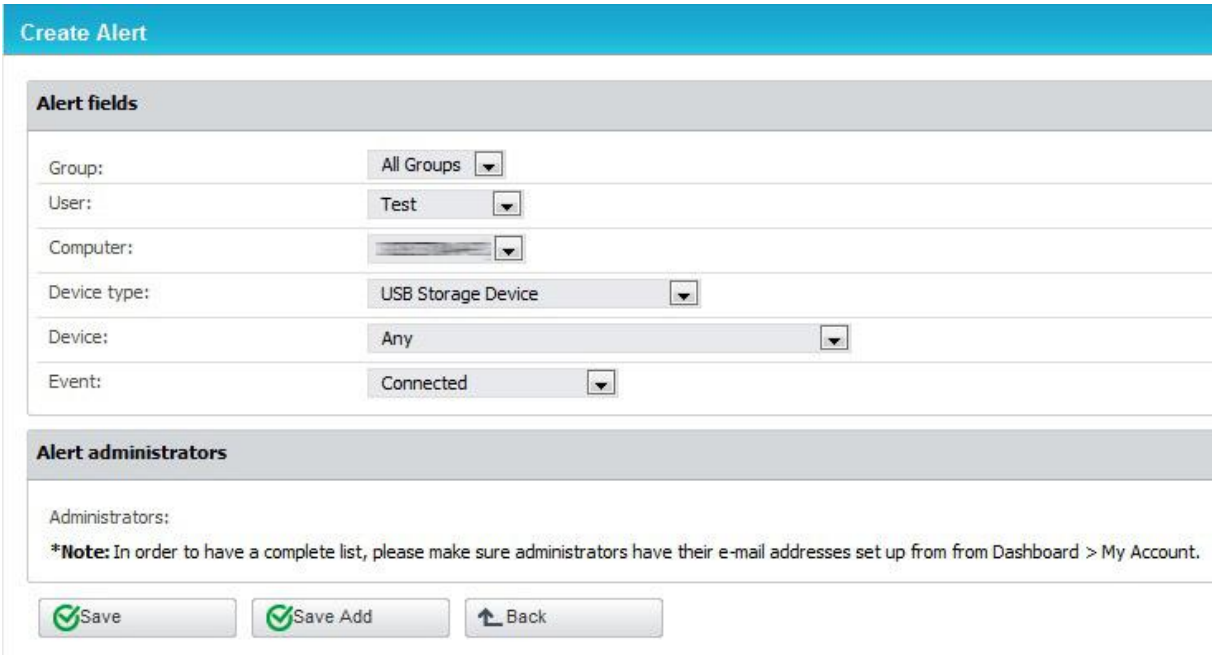
Note!

Both the APNS Certificate and Update and Support system alerts can be disabled from General Dashboard -> System Status

9.2. Define Alerts (Device Control Alerts)



To create a new alert, go to “Define Alerts” and click “Create”.



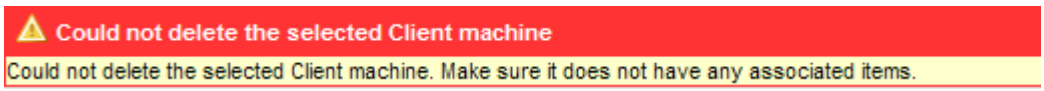
Then select the Group, Client, Computer, Device type or Device - depending if you mean a single device or all devices of a certain type - and the event that will trigger the notification. The filter is designed to make finding information quick and easy.

You can also select one or more administrators to receive the same notification(s). This is useful in case there is more than one administrator for Endpoint Protector.

Example: if you want to be notified when a certain device is connected to a certain computer you must set up an alert choosing the specific device and computer that you wish to be notified of and selecting the "Connected" event from the events list.

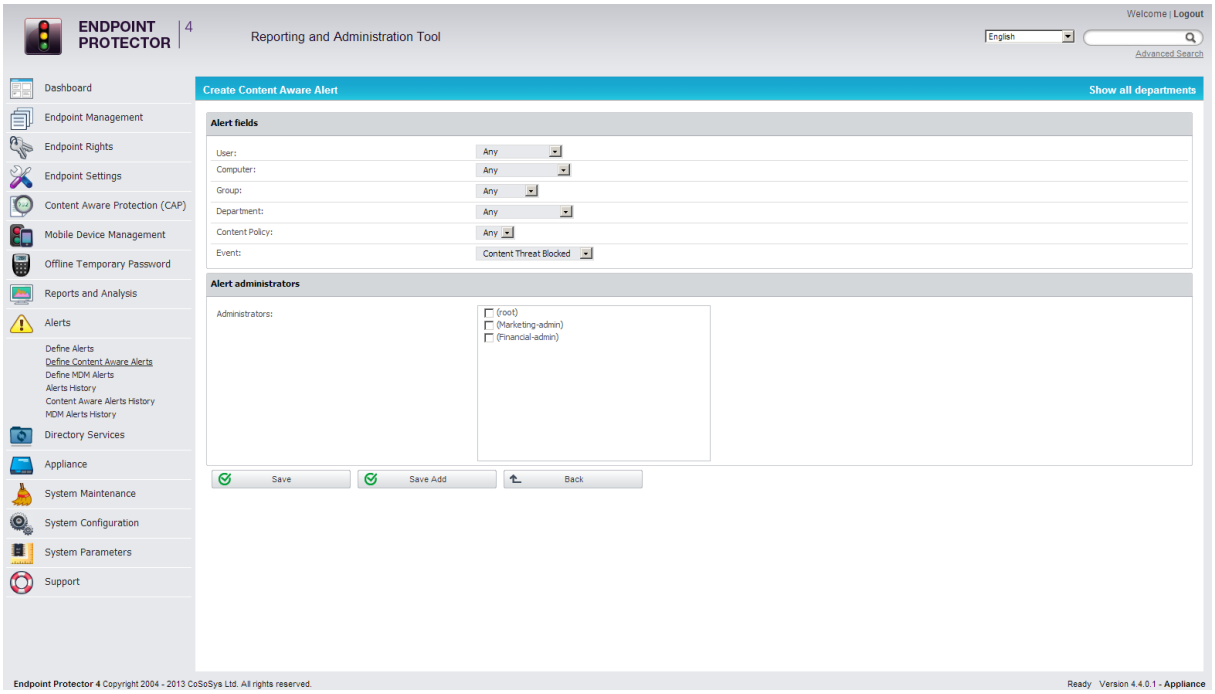
In this case, the "Client" and "Group" fields do not influence the triggering of the alert so there is no need to fill them out. Setting up a value for the "Group" field means that the alert will be triggered when the selected event occurs for any clients or computers in that group.

If you try to delete any items (Users, Groups, Computers etc.) that have been used in setting up an alert, you will receive a notification, and you will not be able to delete them.


Could not delete the selected Client machine
Could not delete the selected Client machine. Make sure it does not have any associated items.

9.3. Define Content Aware Alerts

To create a new Content Aware Alert corresponding to the policies defined in the Content Aware Protection module, go to Define Content Aware Alerts submenu option and click “Create”.



Then select the Group, Client, Computer, User that you want to monitor, the Content Aware Policy to be considered, and the event that will trigger the notification. The filter is designed to make finding information quick and easy.

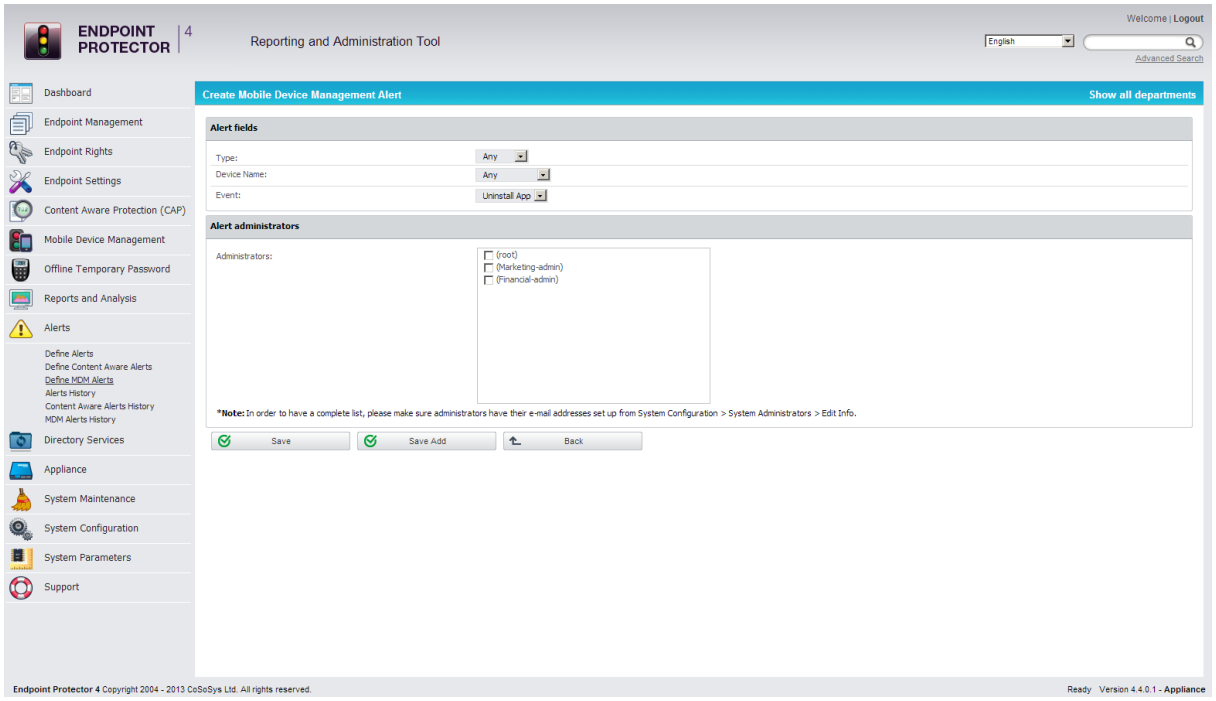
Example: if you want to be notified when a file containing credit card information is attached to an E-MAIL on one of the Financial Departments computers, you must set up an alert choosing the Financial Department as the monitored entity, the Content Aware Policy that inspects documents for that type of information and, finally, selecting the “Content Threat Detected” event from the events list.

Note!

Before creating the alert, you must make sure that the selected Content Aware Policy is enabled on the chosen Computer, User, Group or Department.

9.4. Define MDM Alerts

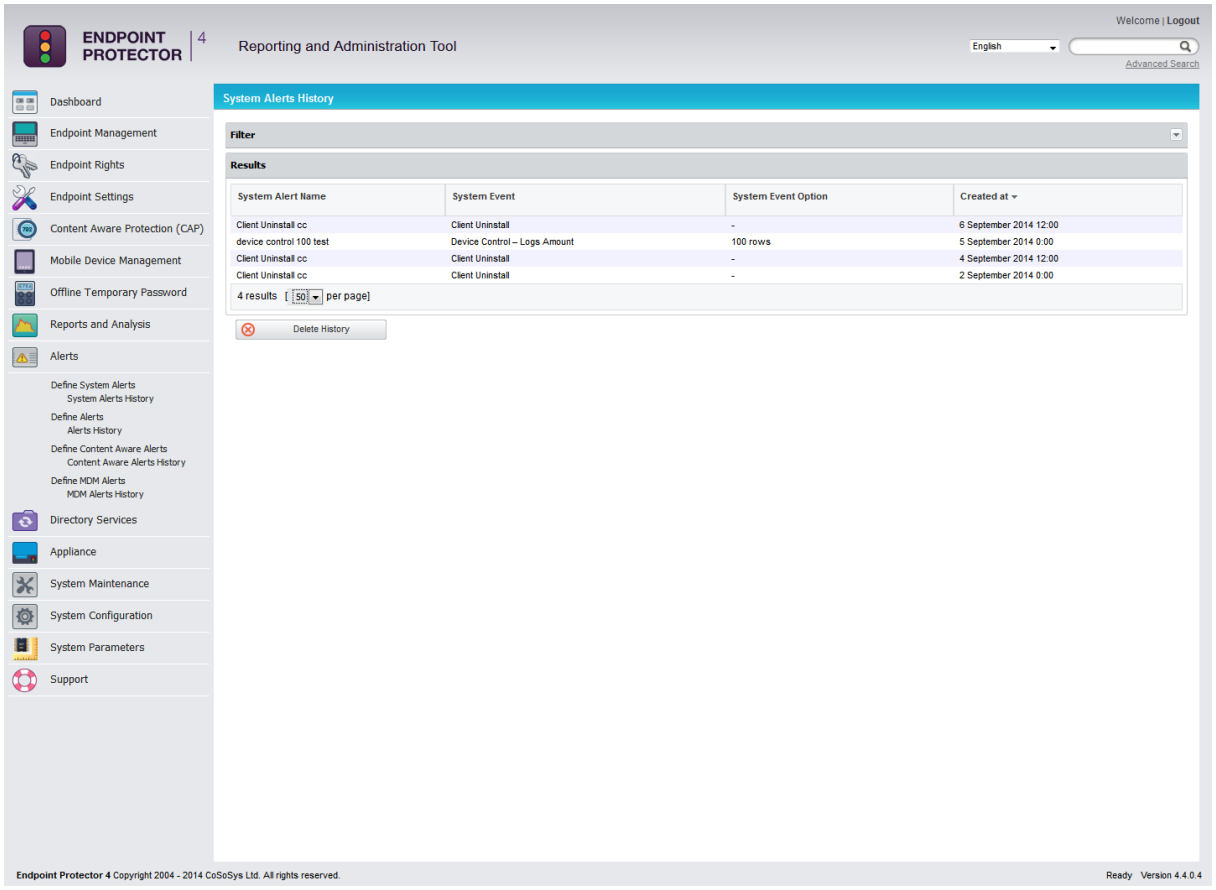
To create a new MDM alert go to the “Define MDM Alerts” tab and press the “Create” button.



Alerts can be created for IOS MDM profile removal, Android application removal, SIM card changed and carrier changed.

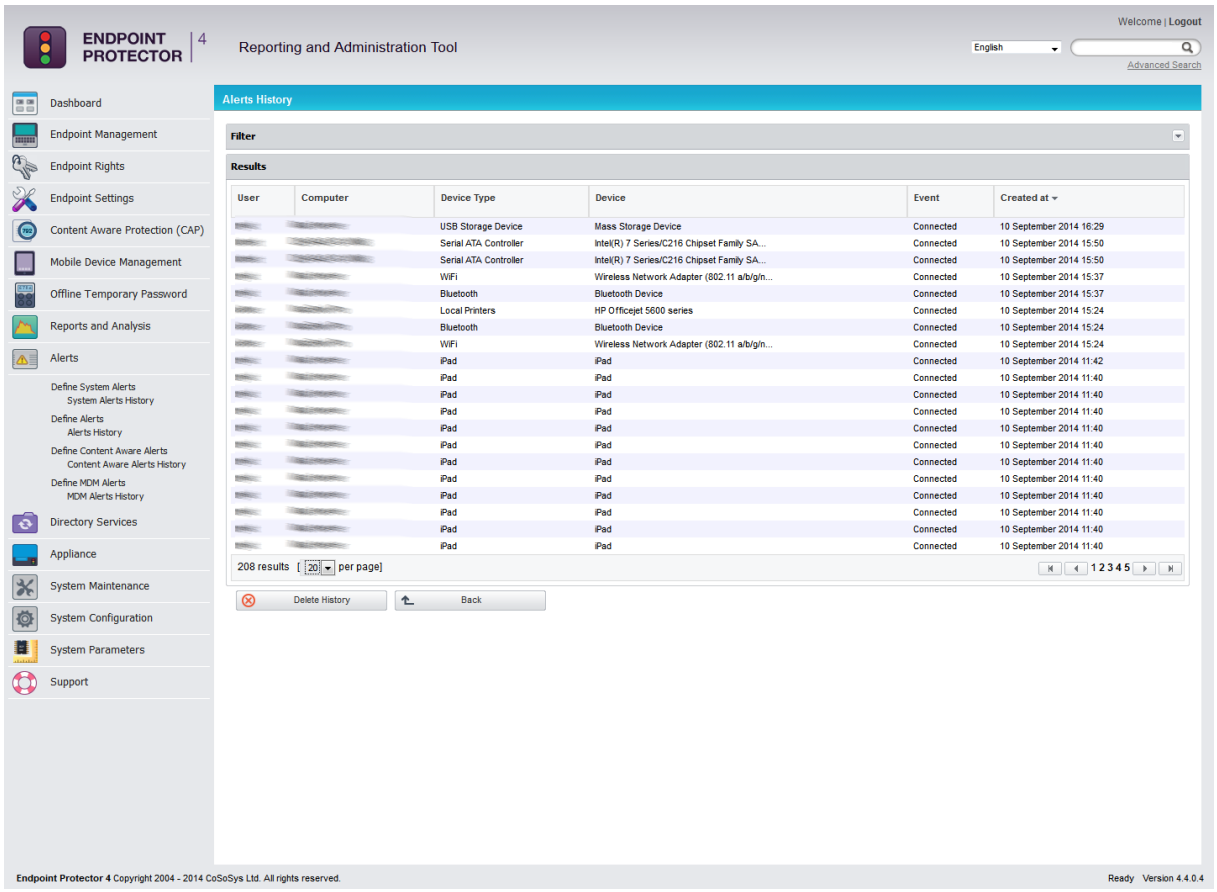
9.5. System Alerts History

A history of the system alerts is kept in this tab for later auditing. Each event that triggers a system alert will be saved here. Administrators can search for data more easily with the implemented filter, while if not needed anymore the logs can be deleted by pressing the “Delete History” button.



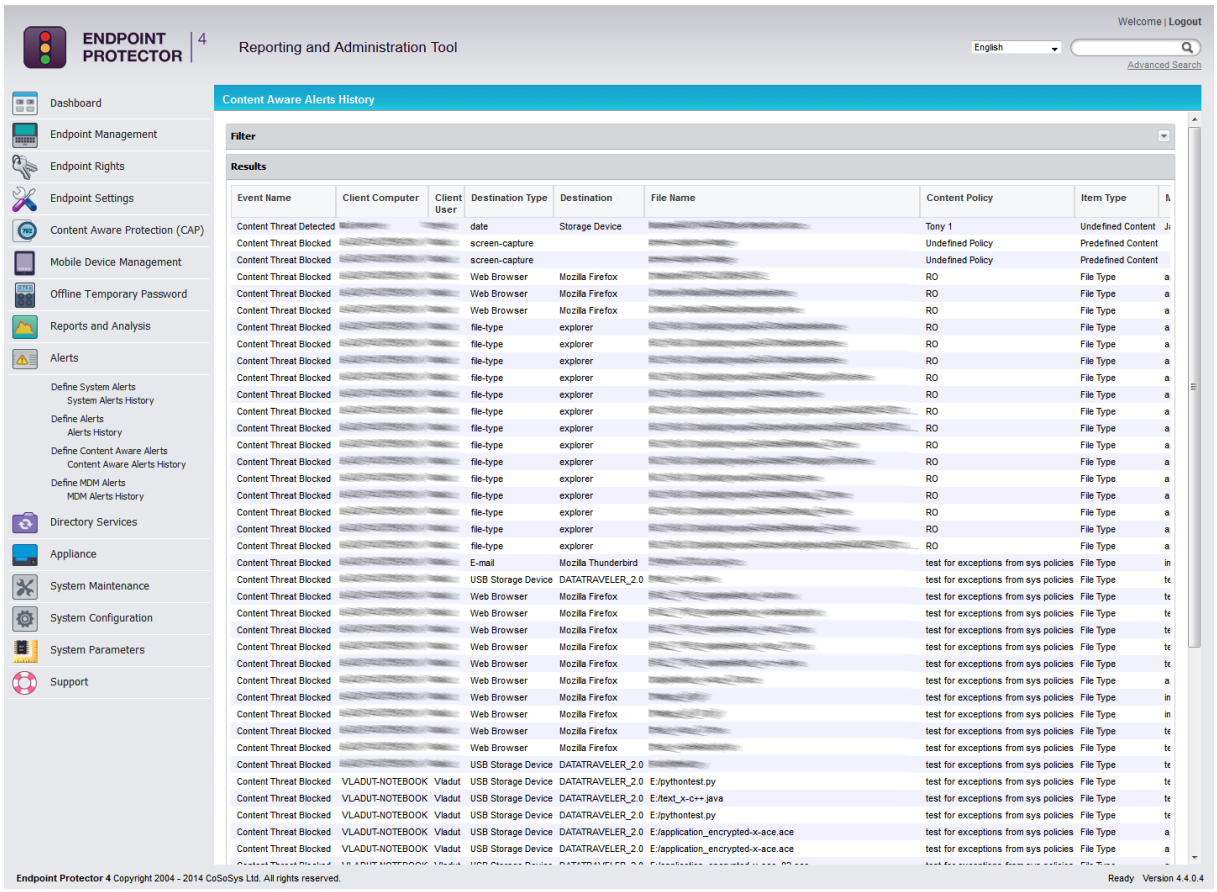
9.6. Alerts History

A history of the alerts is kept in this tab for later auditing. Each event that triggers an alert will be saved here. Administrators can search for data more easily with the implemented filter, while if not needed anymore the logs can be deleted by pressing “Delete History” the button.



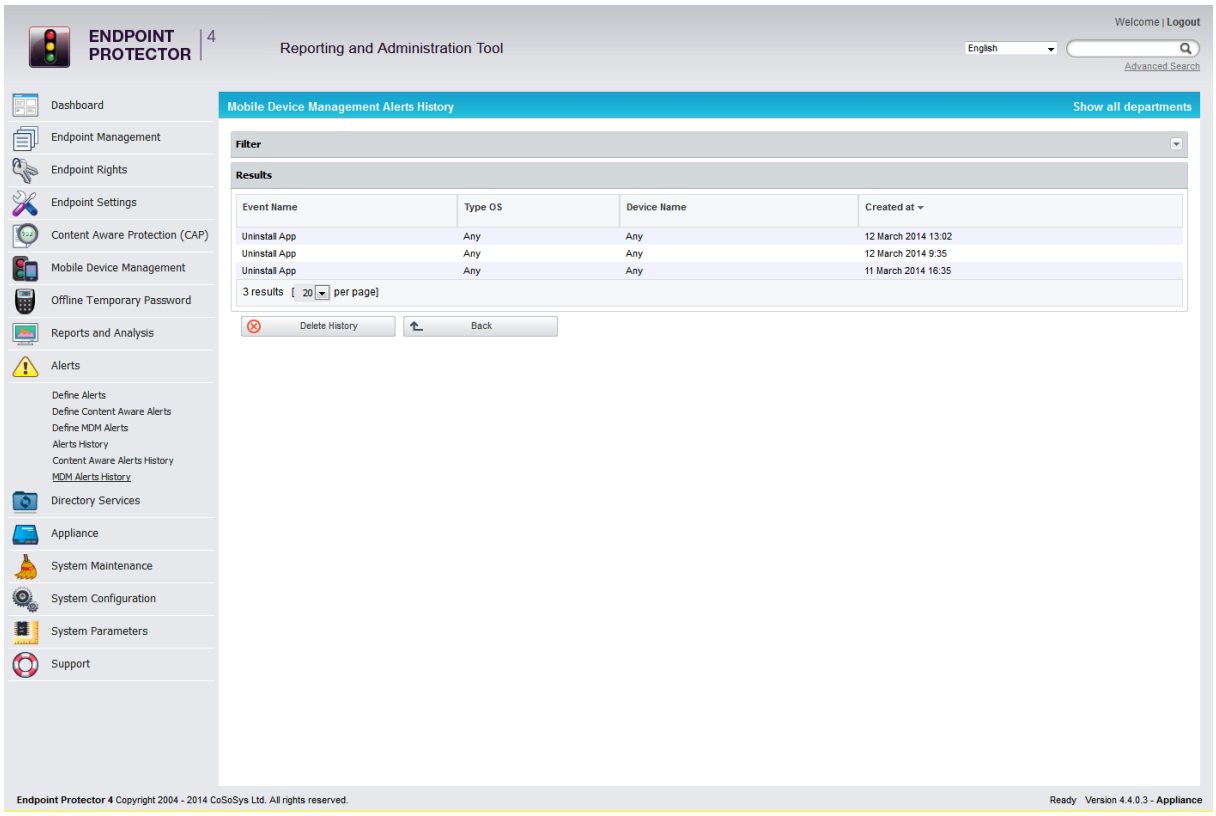
9.7. Content Aware Alerts History

A history of the content aware alerts is kept in this tab for later auditing. Each event that triggers a content aware alert will be saved here. Administrators can search for data more easily with the implemented filter, while if not needed anymore the logs can be deleted by pressing the "Delete History" button.



9.8. MDM Alerts History

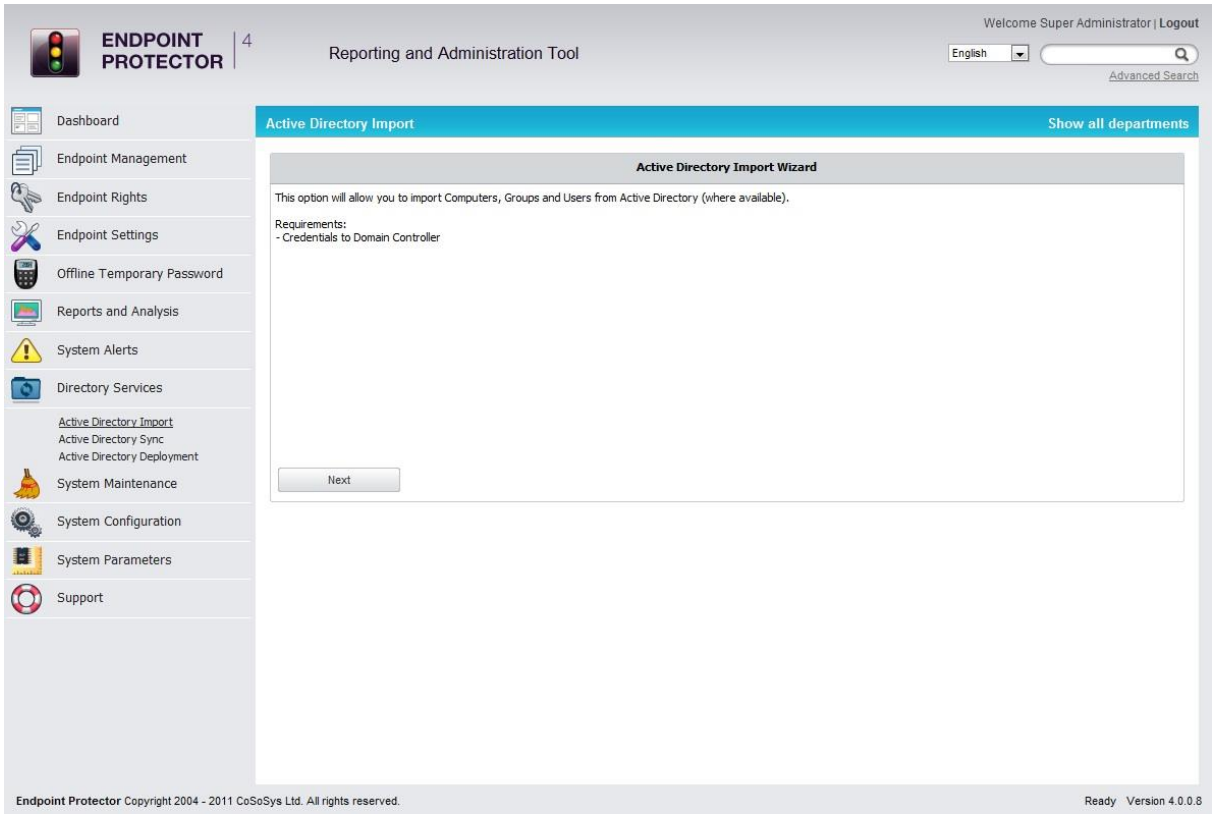
A history of the MDM alerts is kept in this tab for later auditing. Each event that triggers an MDM alert will be saved here. Administrators can search for data more easily with the implemented filter, while if not needed anymore the logs can be deleted by pressing the “Delete History” button.



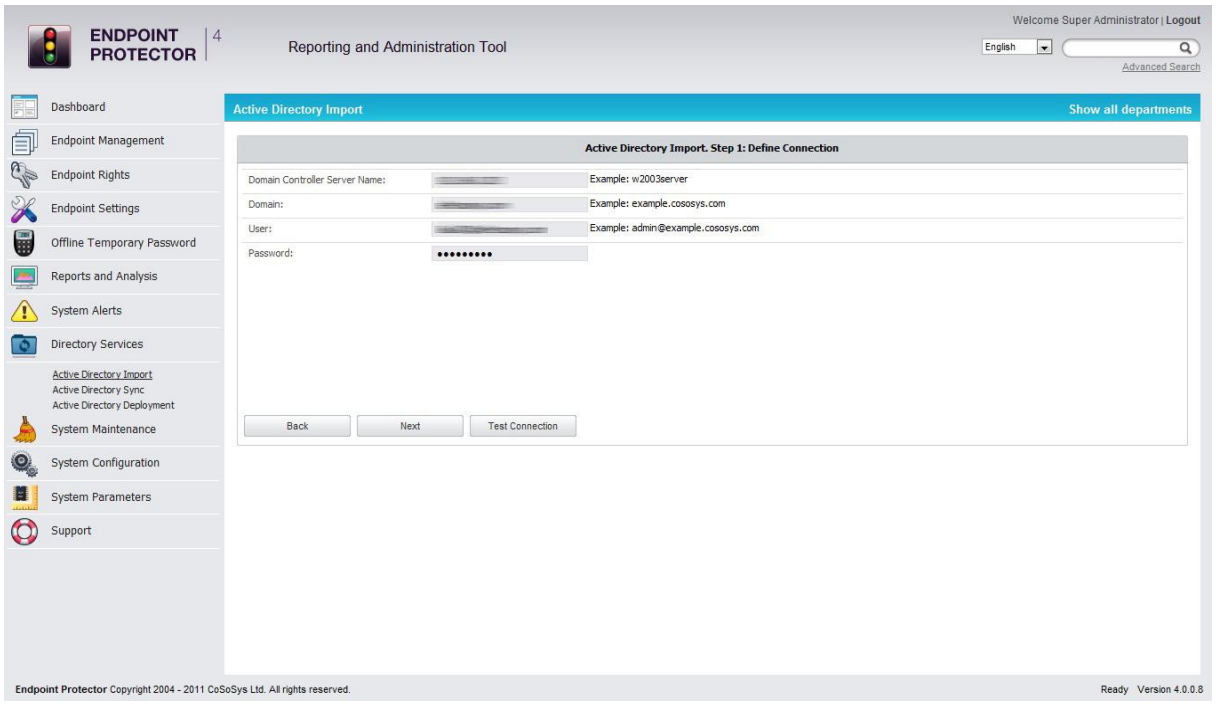
10. Directory Services

10.1. Active Directory Import

This module allows you to import Computers, Groups and Users from Active Directory (where available).



If you have the requirements, simply click “Next”.

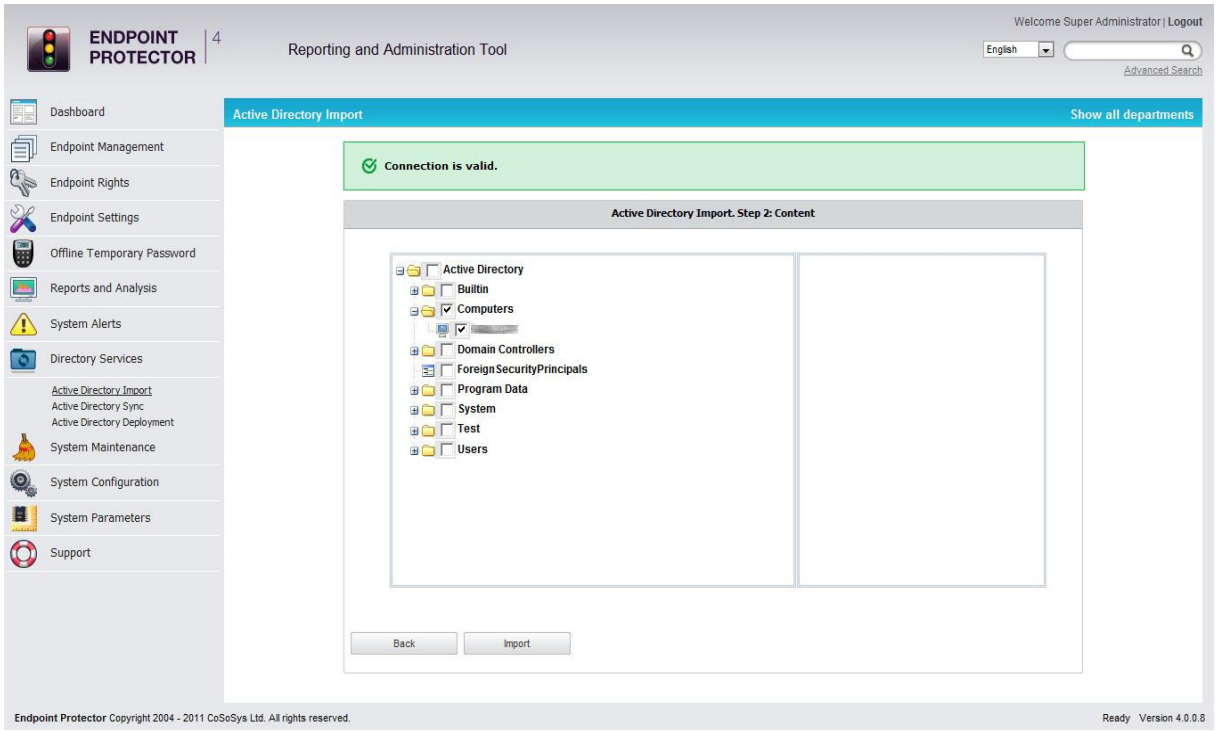


Enter the Active Directory domain controller server name, the domain name and a username and password in the format as in the examples presented in the form. First, you can push the “Test Connection” button to test if the connection is established successfully. If the connection is valid, push the “Next” button. This operation might take some time, depending on the volume of data that needs to be imported.

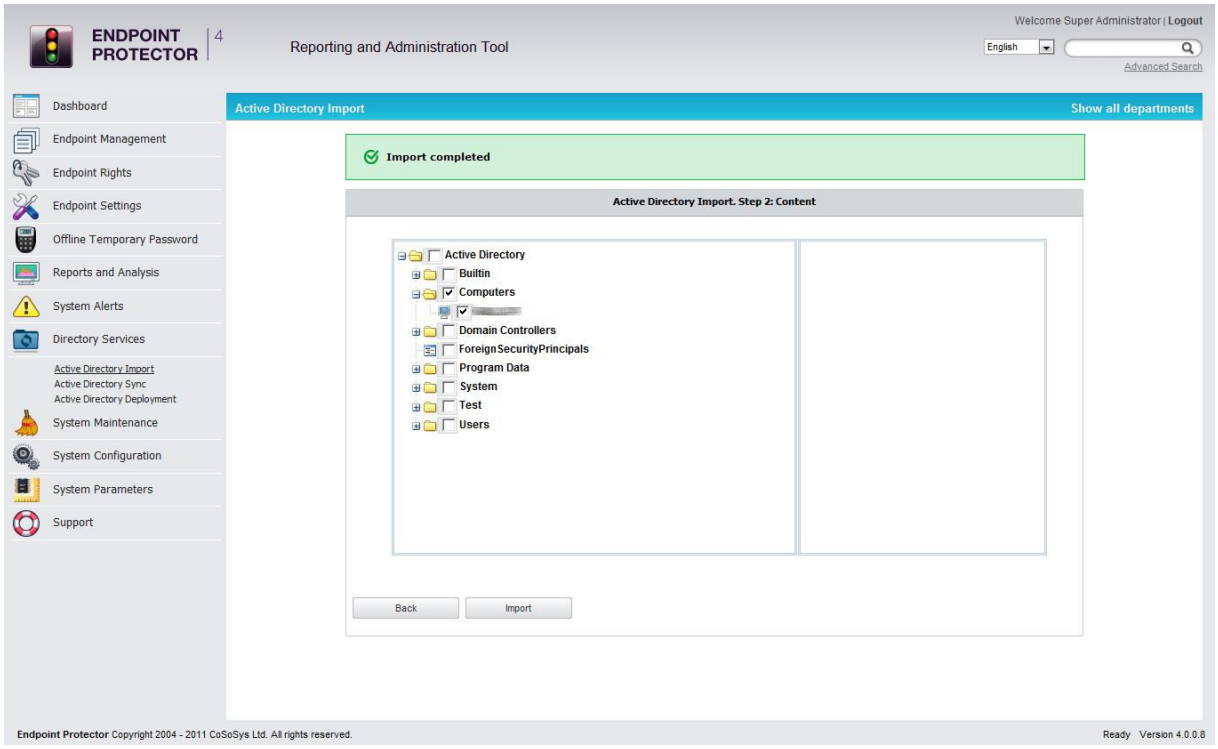
Note!

When having to import a very large number of entities from the Active Directory, we recommend using the "Domain/Search In" filter from the AD Import page in order to get only the relevant information displayed for import. Due to browser limitations, importing the whole AD structure may impede the display of the import tree if it contains a very large number of entities.

In the next step, simply select what items you would like to import by clicking the checkbox next to them and finally, select "Import".



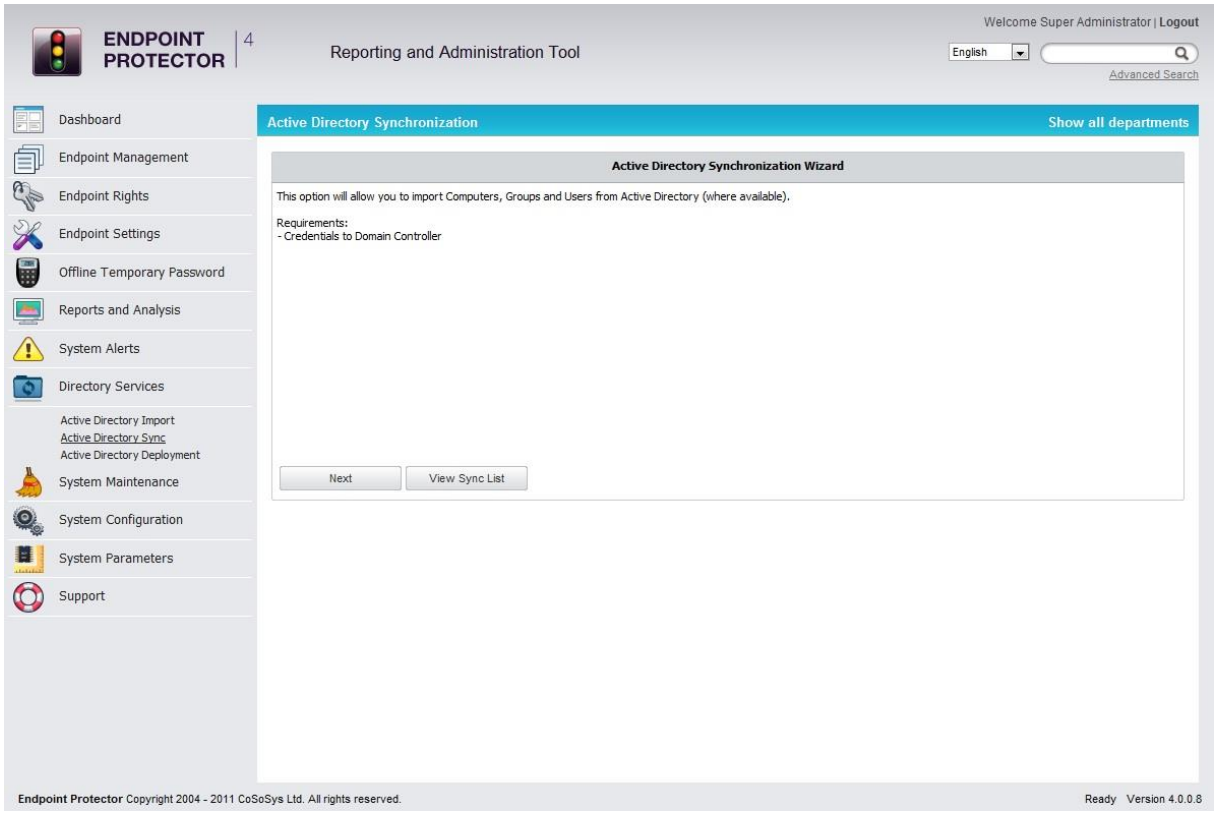
If the import procedure was successful, you will see the message "Import completed".



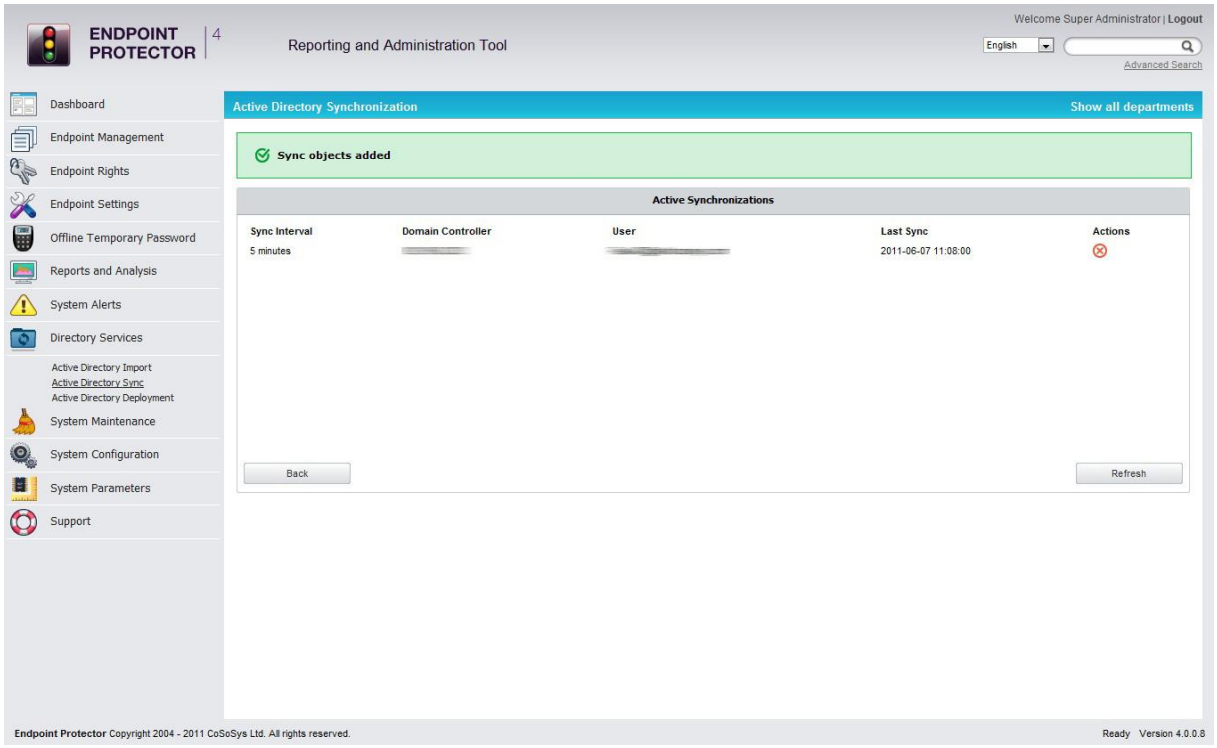
10.2. Active Directory Sync

Special requirements: Endpoint Protector Timer, or the Windows Scheduler setup to call the synchronization PHP script.

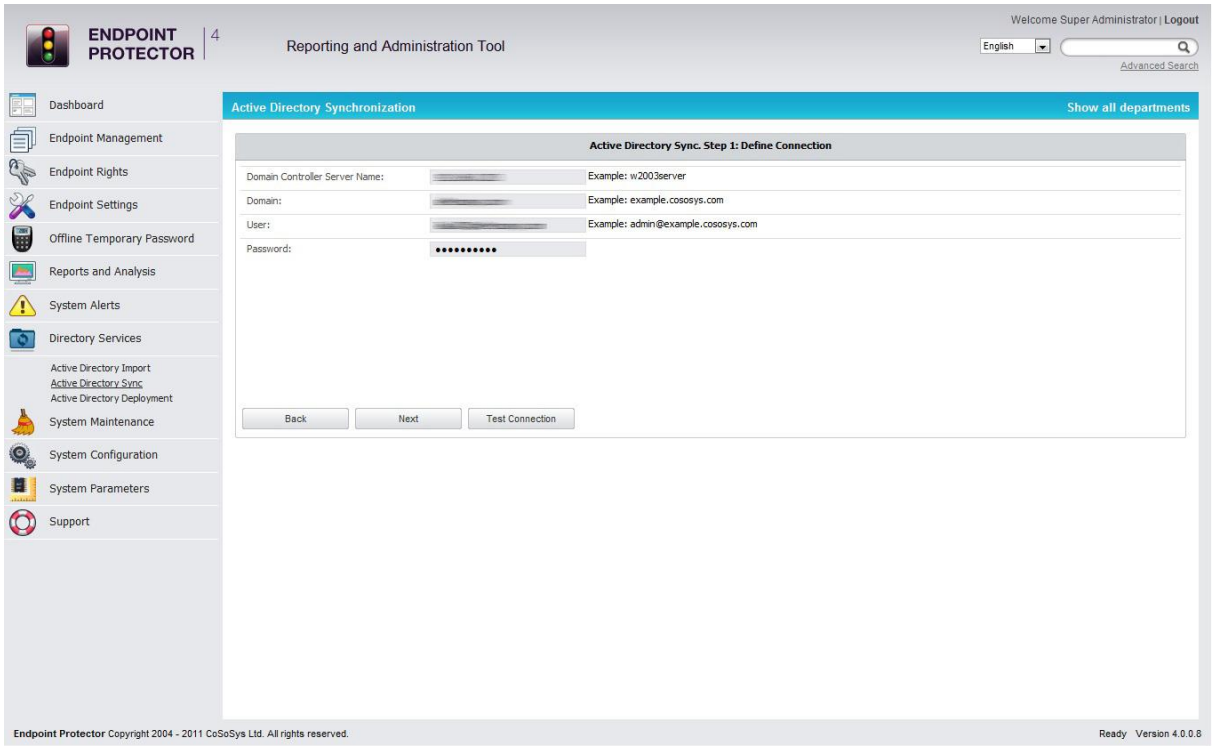
This module allows you to synchronize the entities in Endpoint Protector with the entities in Active Directory (Computers, Users, and Groups).



You can either examine existing synchronizations by clicking the “View Sync List” button,

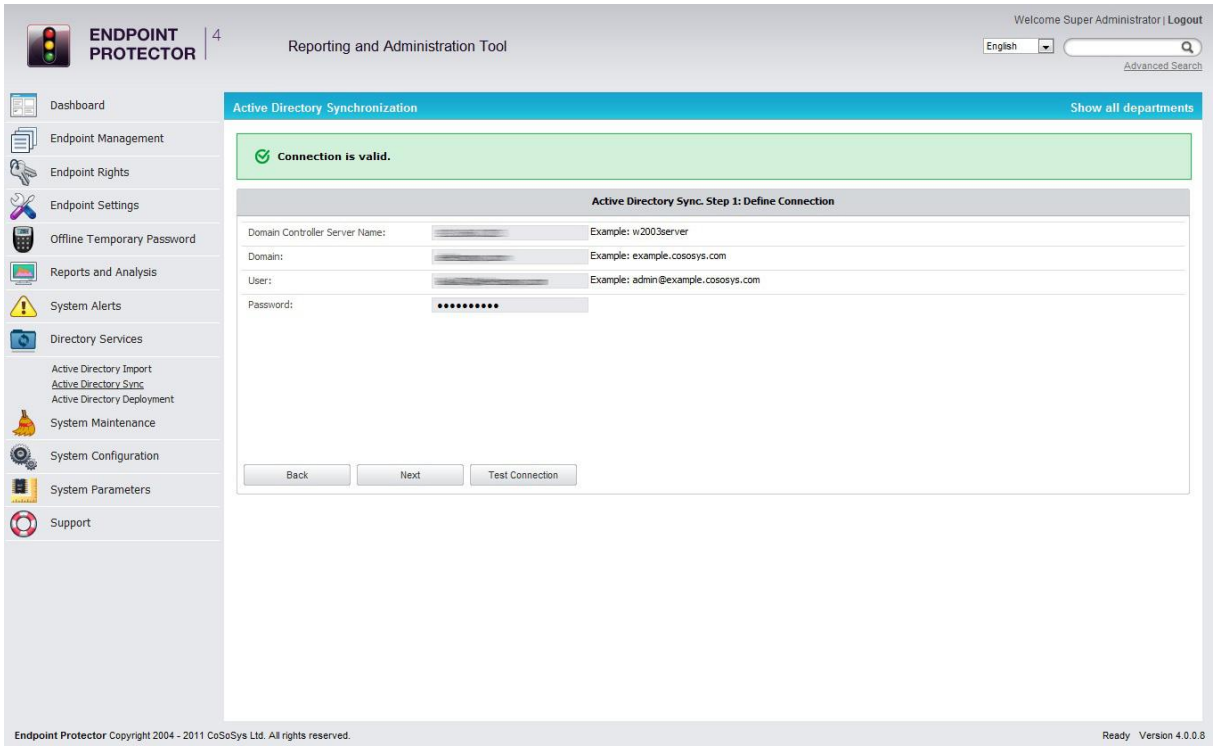


or, if you have the requirements, simply click “Next” to set up your synchronization settings.



Enter the Active Directory domain controller server name, the domain name and a username and password in the format as in the examples presented in the form.

You can also check if your settings are correct by clicking the "Test Connection" button.



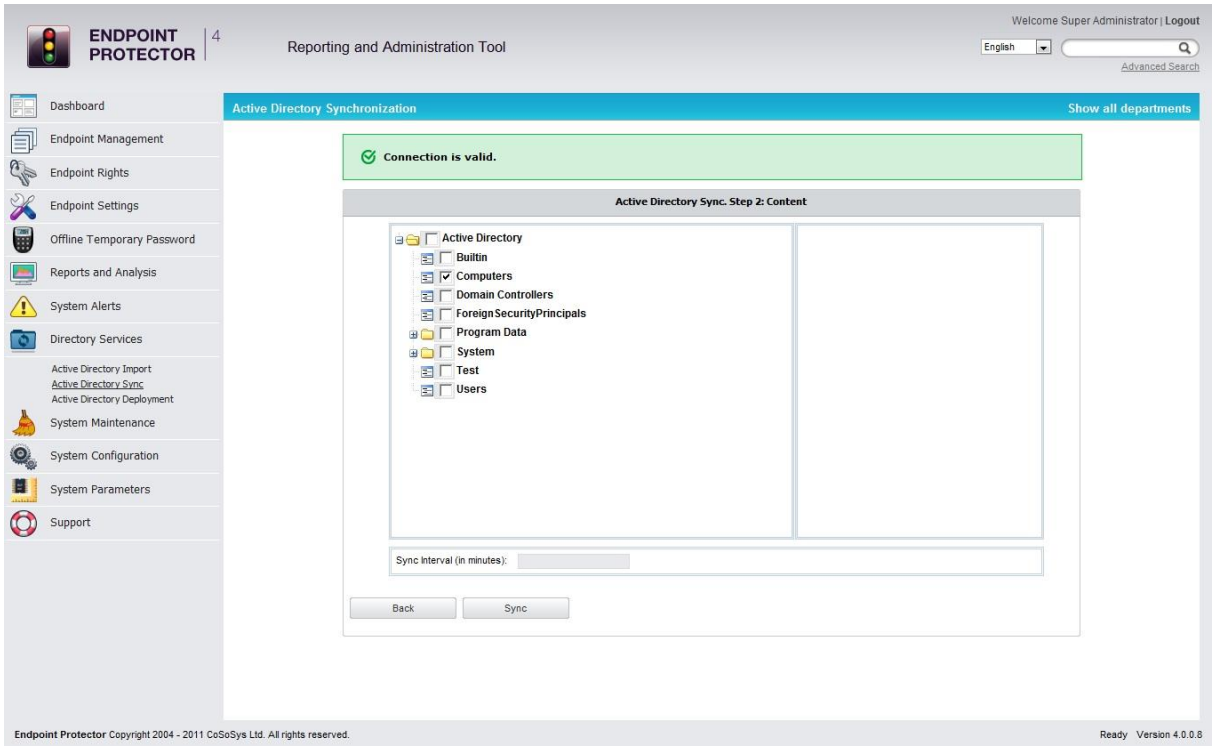
You should see a message "Connection is valid" on the top of the page.

Click "Next" to continue.

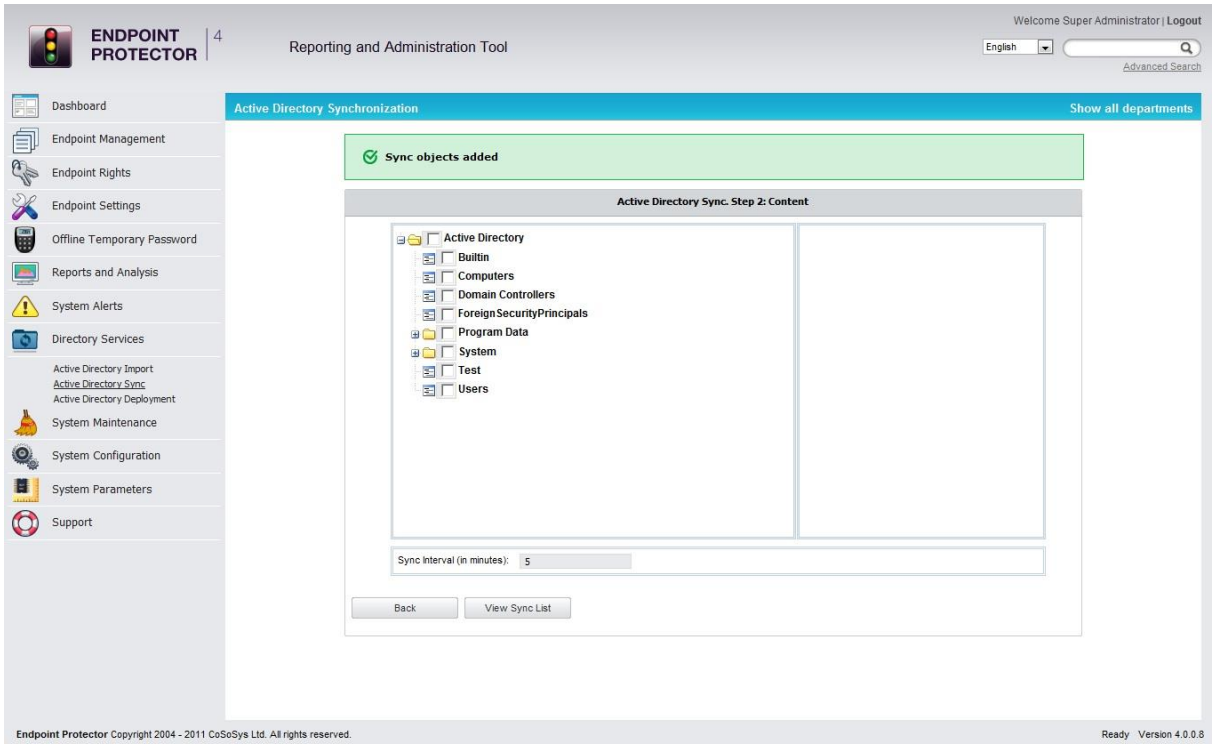
Note!

This operation might take some time, depending on the volume of data that needs to be synchronized.

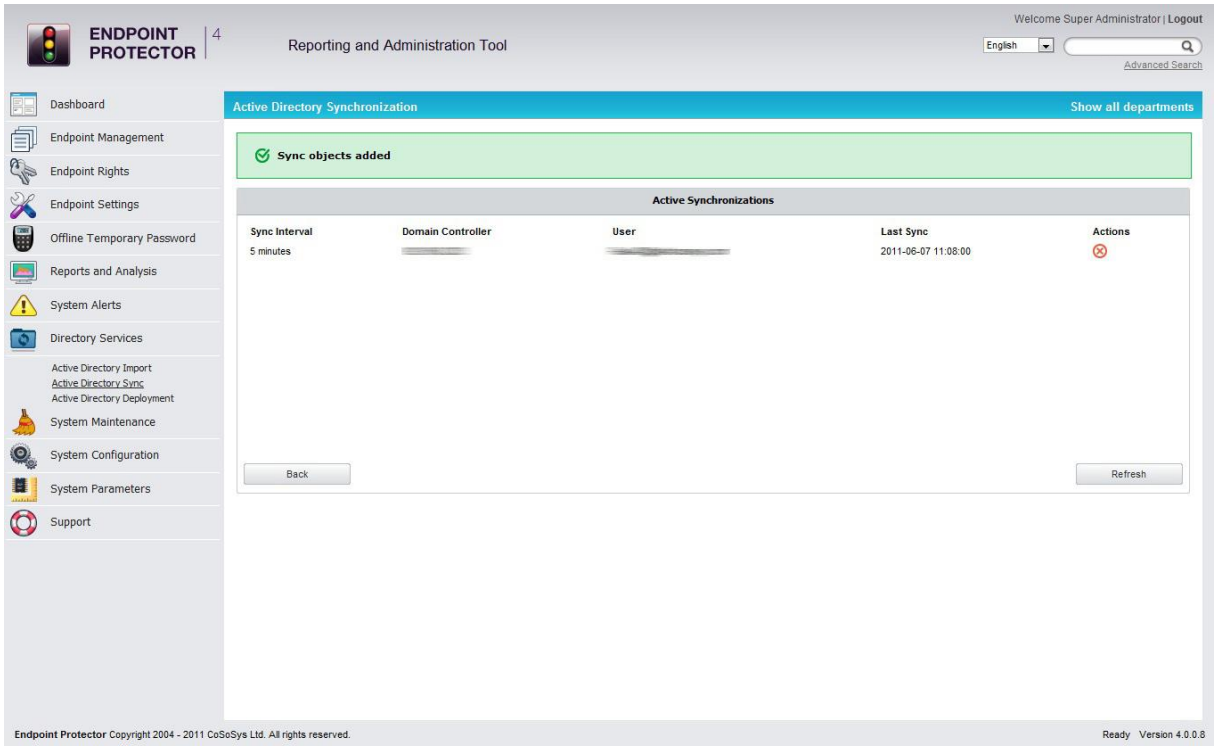
In the next step, simply select what items you would like to synchronize by clicking the checkbox next to them, define a sync interval and select “Sync”.



You will see the message “Sync object added”.



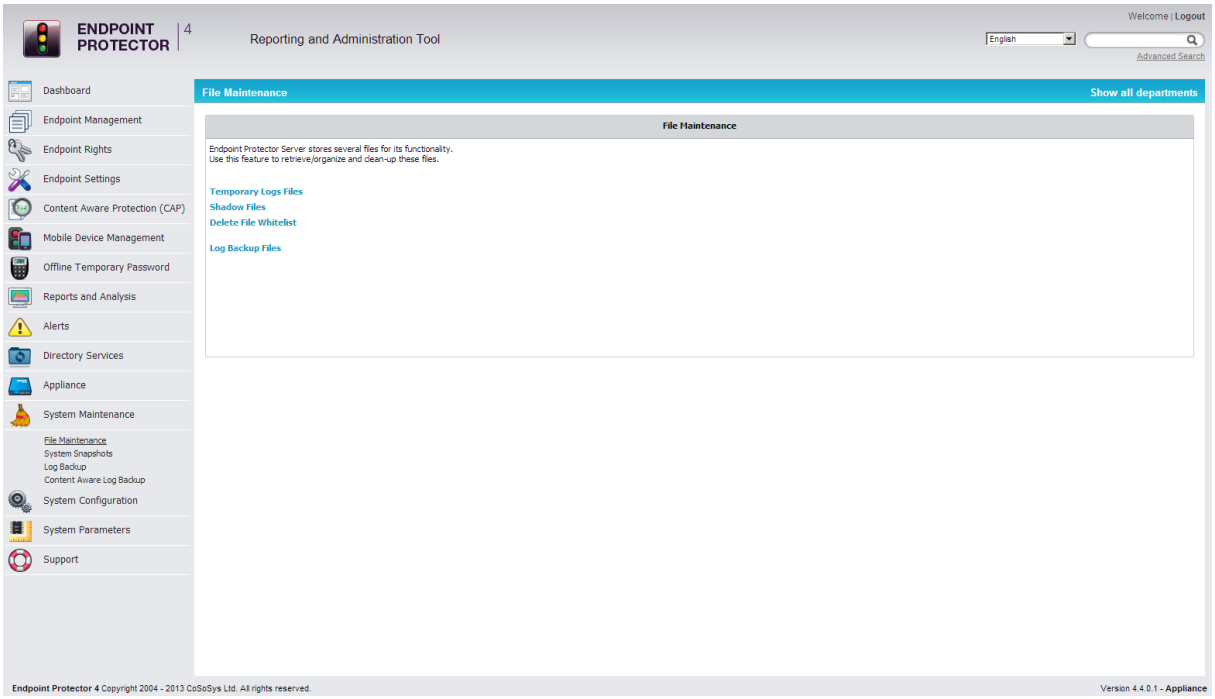
You can set up multiple synchronizations from multiple locations at once. These can be viewed and canceled in the “View Sync List”.



11. System Maintenance

11.1. File Maintenance

This module allows the administrator to retrieve/organize and clean-up files used by Endpoint Protector Server.



The available options are:

- **Temporary Log Files**: allows archiving and deleting log files from a selected client computer
- **Shadow Files**: allows archiving and deleting shadowed files from a selected client computer
- **Log Backup Files**: allows archiving and deleting previously backed up log files

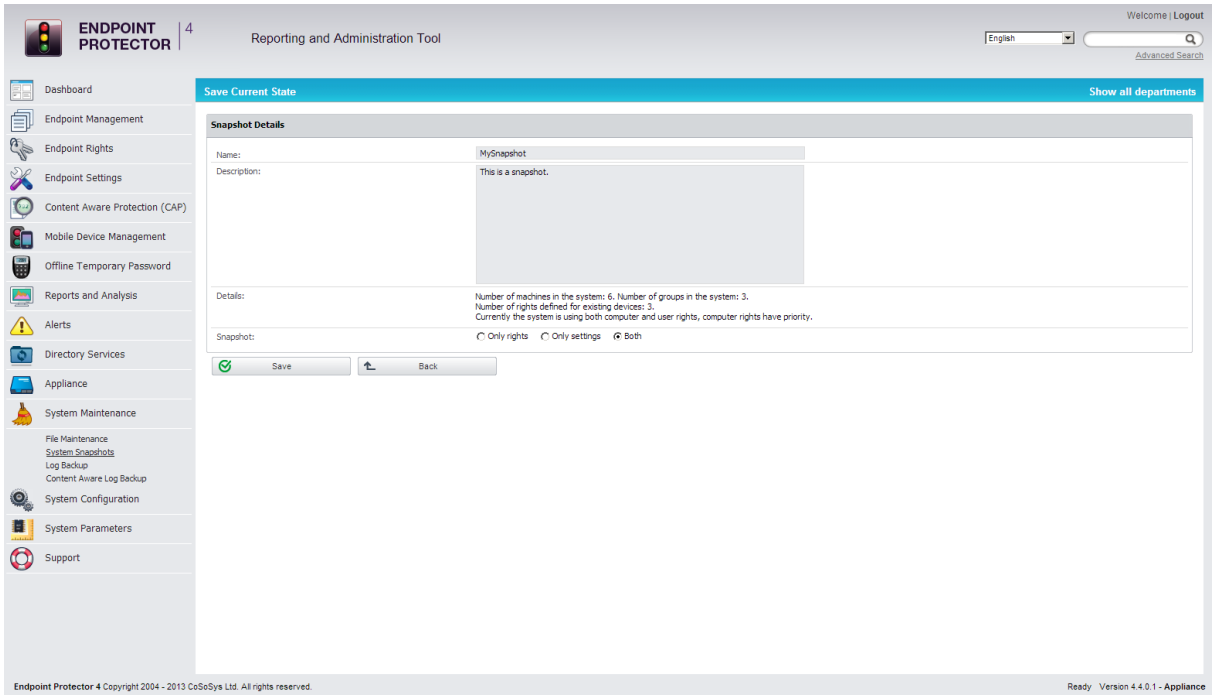
To archive a previously selected set of files, click the "Save as Zip" button, while to permanently remove a set of files from the Endpoint Protector Server use the "Delete" button.

11.2. System Snapshots

The System Snapshots module allows you to save all device control rights and settings in the system and restore them later, if needed.

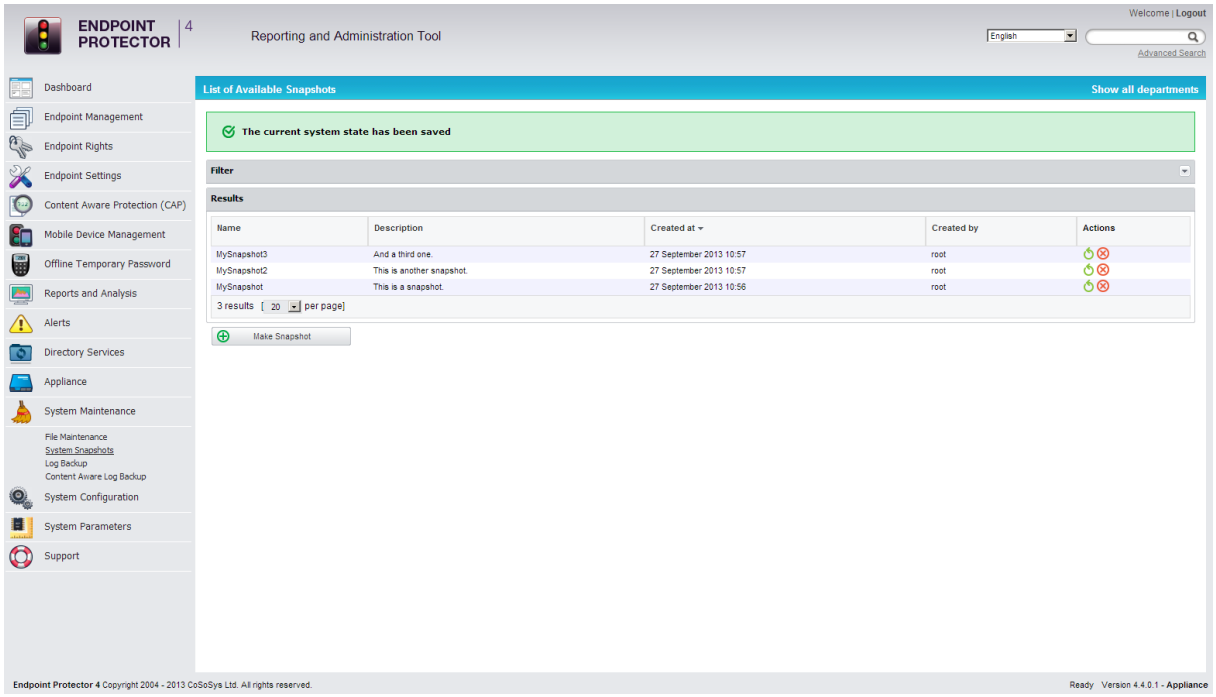
After installing the Endpoint Protector 4 Server, we strongly recommend that you create a System Snapshot before modifying anything. In this case you can revert back to the original settings if you configure the server incorrectly.

To create a System Snapshot, access the module from System Configuration and click "Make Snapshot".



Enter a name for the snapshot, and a description. Select also what you wish to store in the snapshot, Only Rights, Only Settings, or Both.

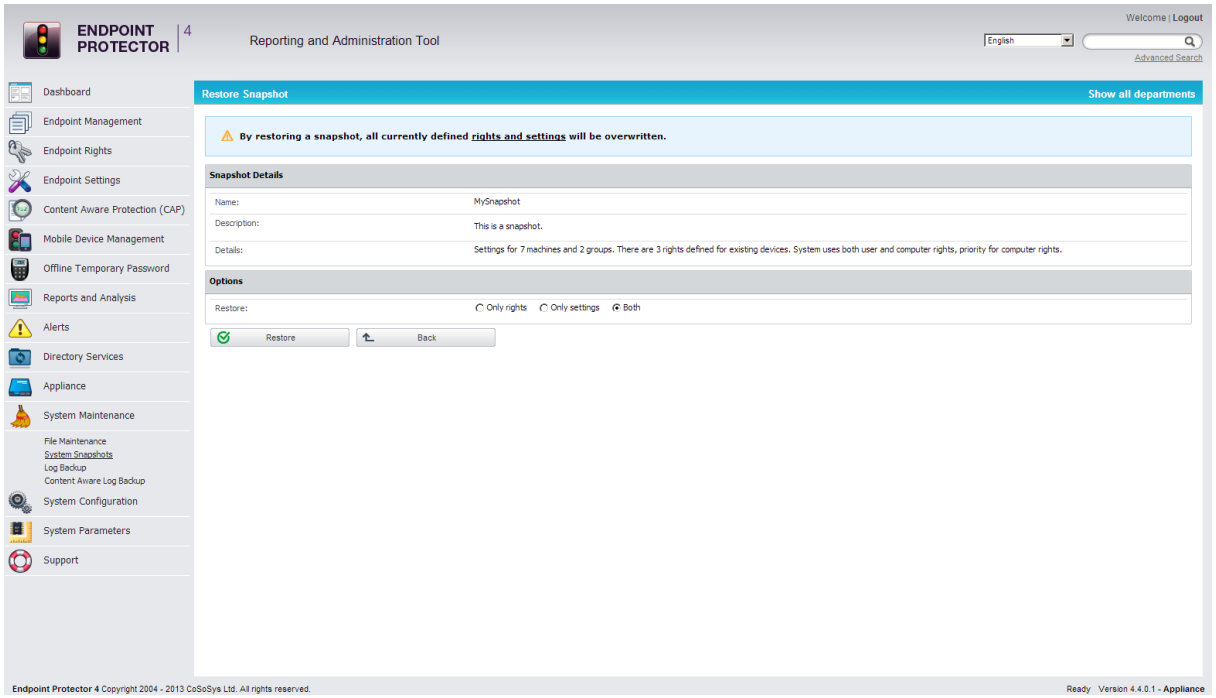
Finally, click "Save".



Your snapshot will appear in the list of System Snapshots.

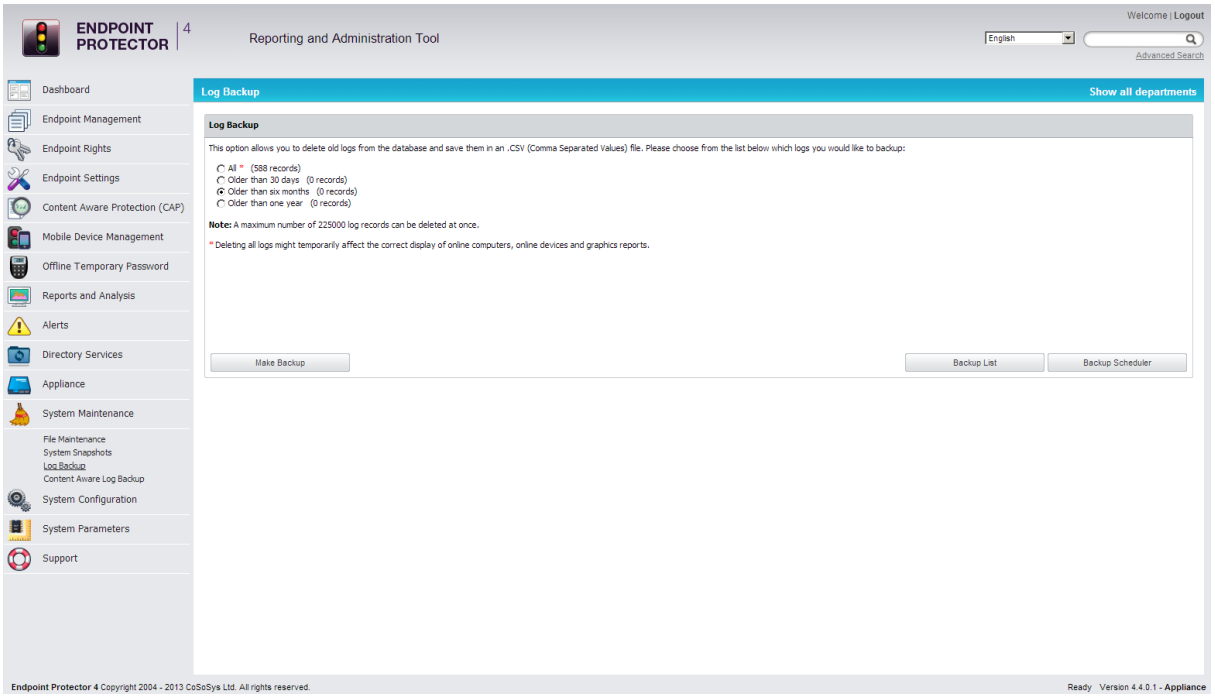
To restore a previously created snapshot click the “Restore” button next to the desired snapshot. - Restore

Confirm restoration by clicking the “Restore” button again in the next window.

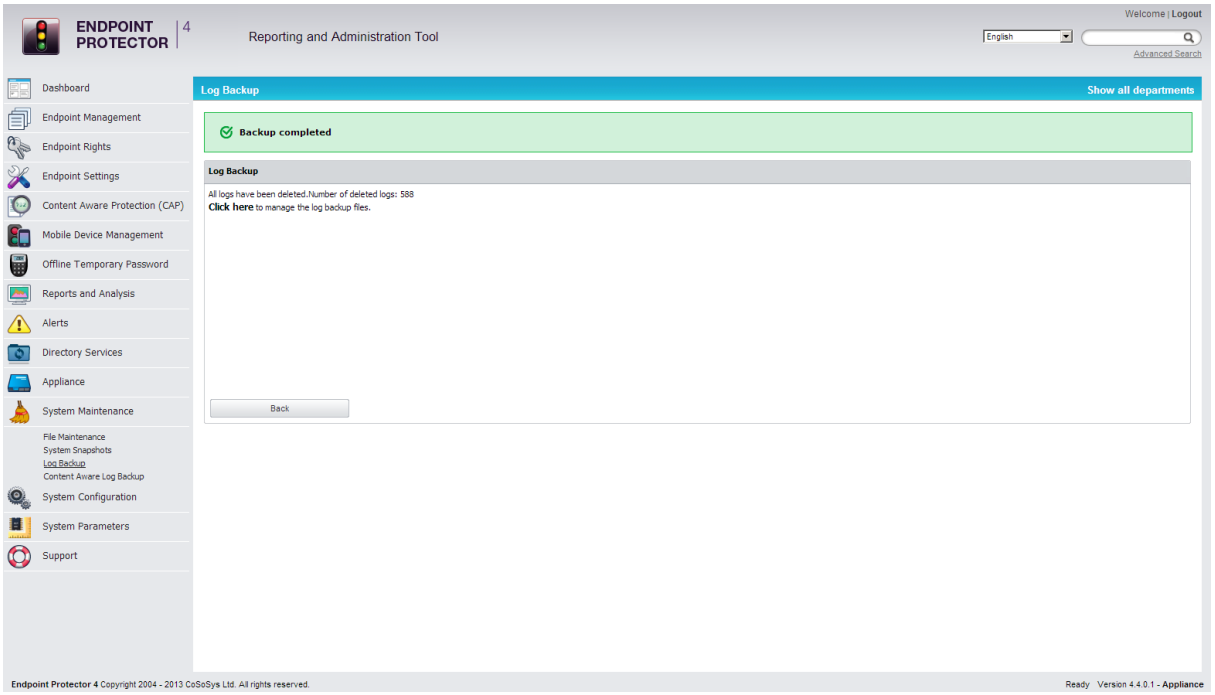


11.3. Log Backup

This module allows you to delete old logs from the database and save them in a .CSV document.


ENDPOINT PROTECTOR 4
Reporting and Administration Tool
Welcome | Logout
English
Advanced Search
Dashboard
Endpoint Management
Endpoint Rights
Endpoint Settings
Content Aware Protection (CAP)
Mobile Device Management
Offline Temporary Password
Reports and Analysis
Alerts
Directory Services
Appliance
System Maintenance
File Maintenance
System Snapshots
Log Backup
Content Aware Log Backup
System Configuration
System Parameters
Support
Log Backup
Show all departments
Log Backup
This option allows you to delete old logs from the database and save them in an .CSV (Comma Separated Values) file. Please choose from the list below which logs you would like to backup:
All * (588 records)
Older than 30 days (0 records)
Older than six months (0 records)
Older than one year (0 records)
Note: A maximum number of 225000 log records can be deleted at once.
* Deleting all logs might temporarily affect the correct display of online computers, online devices and graphics reports.
Make Backup
Backup List
Backup Scheduler
Endpoint Protector 4 Copyright 2004 - 2013 CoSoSys Ltd. All rights reserved.
Ready Version 4.4.0.1 - Appliance

Here you can select the logs you wish to back-up. Simply select an option and click “Make Backup”.

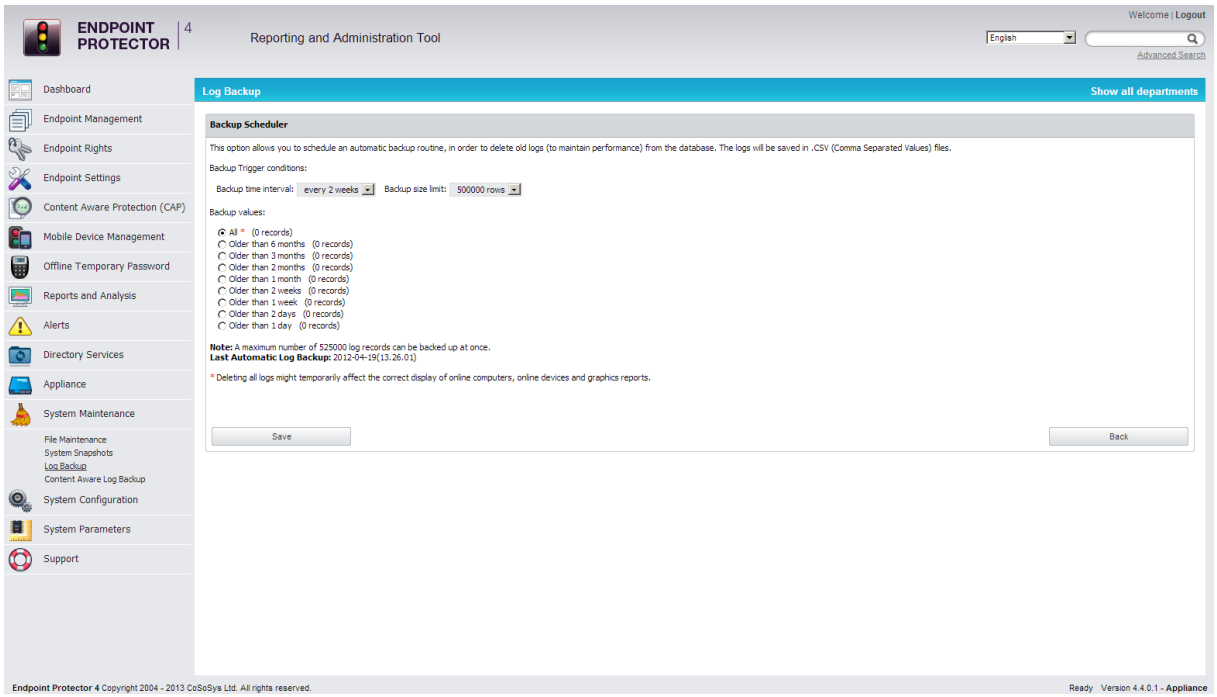


You should see the message “Backup Completed” in the top-center of your browser.

You can download and view the logs by selecting the “click here” link.

11.3.1. Backup Scheduler (Automatic Log Backup)

You can back up your log files also automatically by using the Backup Scheduler option.


ENDPOINT PROTECTOR 4
Reporting and Administration Tool
Welcome | Logout
English
Advanced Search
Dashboard
Endpoint Management
Endpoint Rights
Endpoint Settings
Content Aware Protection (CAP)
Mobile Device Management
Offline Temporary Password
Reports and Analysis
Alerts
Directory Services
Appliance
System Maintenance
File Maintenance
System Snapshots
Log Backup
Content Aware Log Backup
System Configuration
System Parameters
Support
Log Backup
Show all departments
Backup Scheduler
This option allows you to schedule an automatic backup routine, in order to delete old logs (to maintain performance) from the database. The logs will be saved in .CSV (Comma Separated Values) files.
Backup Trigger conditions:
Backup time interval: every 2 weeks
Backup size limit: 500000 rows
Backup values:
All * (0 records)
Older than 6 months (0 records)
Older than 3 months (0 records)
Older than 2 months (0 records)
Older than 1 month (0 records)
Older than 2 weeks (0 records)
Older than 1 week (0 records)
Older than 2 days (0 records)
Older than 1 day (0 records)
Note: A maximum number of 525000 log records can be backed up at once.
Last Automatic Log Backup: 2012-04-19(13.26.01)
* Deleting all logs might temporarily affect the correct display of online computers, online devices and graphics reports.
Save
Back
Endpoint Protector 4 Copyright 2004 - 2013 CoSoSys Ltd. All rights reserved.
Ready Version 4.4.0.1 - Appliance

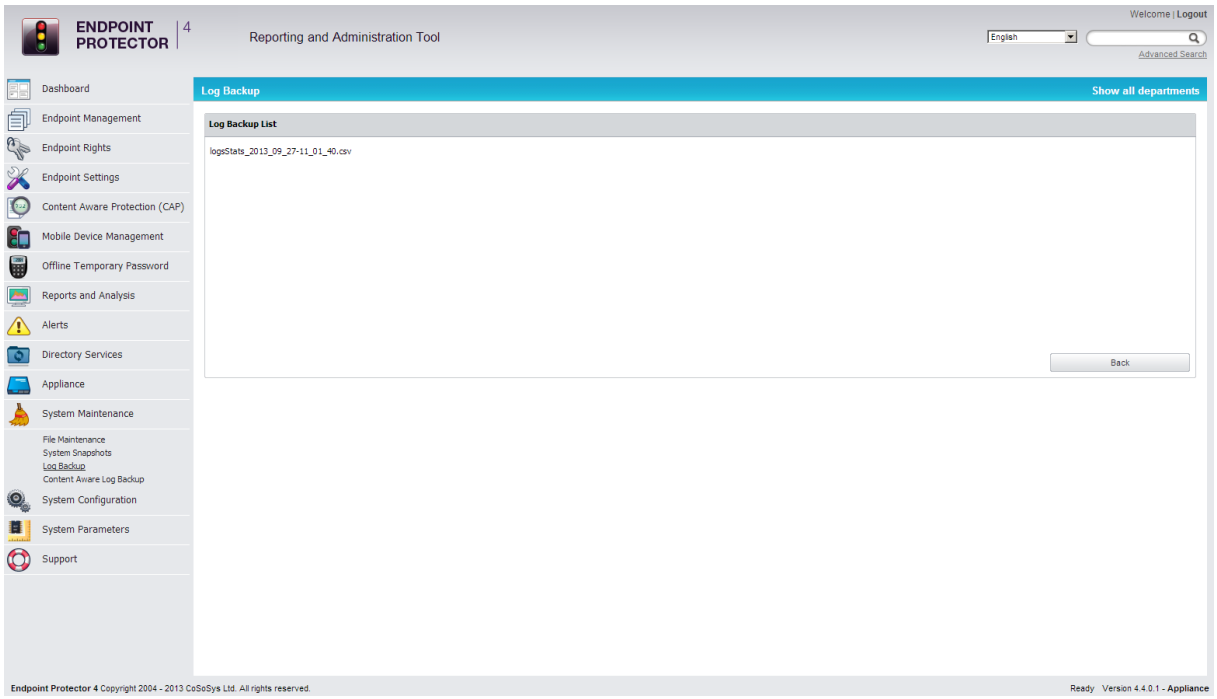
Here you can schedule an automatic backup routine by setting two trigger conditions:

Backup time interval - allows you to select a certain time interval for repeating the backup operation

Backup size limit - allows you to select a maximum size for the logs to be backed up

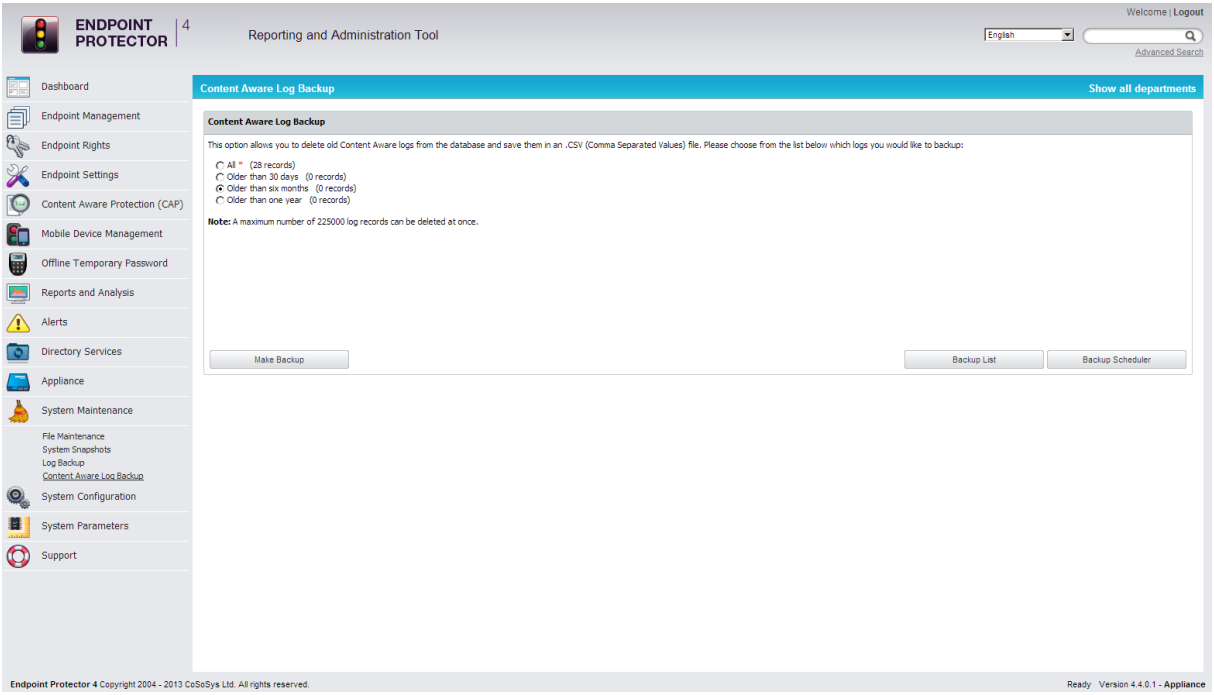
In case that you don't wish to set a specific value for one or both of these options, please leave the specific field(s) blank. After specifying the logs to be backed up automatically based on their creation time, please click "Save" in order for your options to be applied.

You can view the created backups by using the Backup List option.

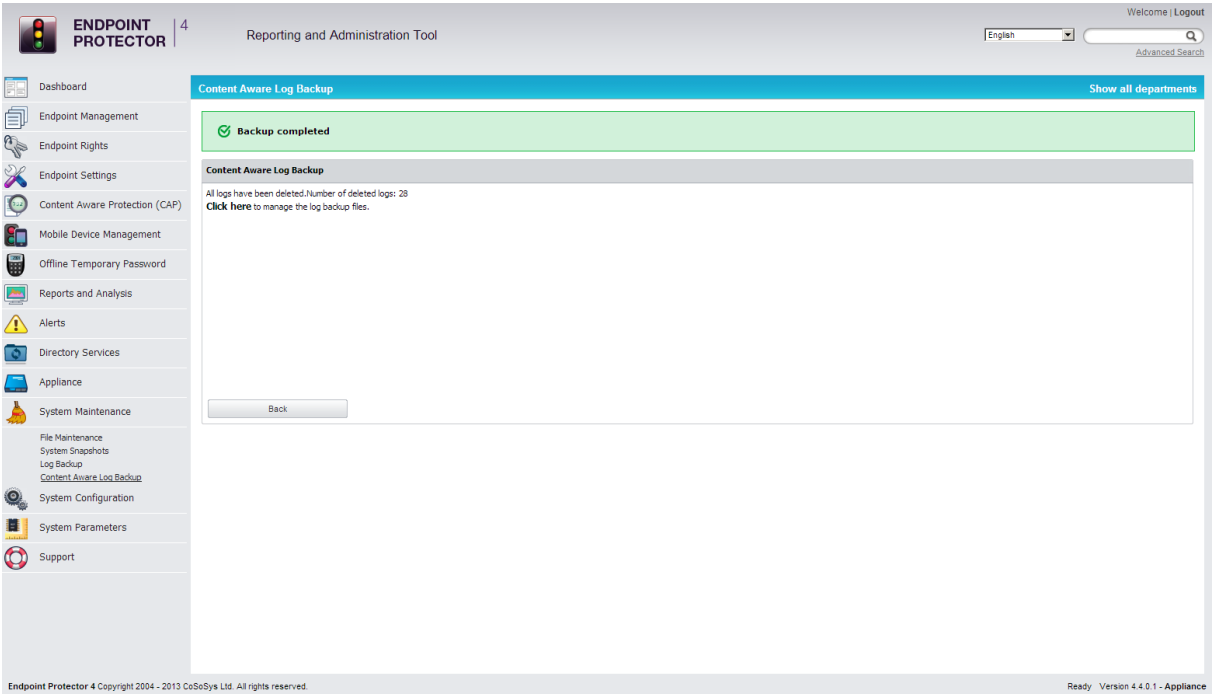


11.4. Content Aware Log Backup

This module allows you to delete old content aware logs from the database and save them in a .CSV document.


ENDPOINT PROTECTOR 4
Reporting and Administration Tool
Welcome | Logout
English
Advanced Search
Dashboard
Endpoint Management
Endpoint Rights
Endpoint Settings
Content Aware Protection (CAP)
Mobile Device Management
Offline Temporary Password
Reports and Analysis
Alerts
Directory Services
Appliance
System Maintenance
File Maintenance
System Snapshots
Log Backup
Content Aware Log Backup
System Configuration
System Parameters
Support
Content Aware Log Backup
Show all departments
Content Aware Log Backup
This option allows you to delete old Content Aware logs from the database and save them in an .CSV (Comma Separated Values) file. Please choose from the list below which logs you would like to backup:
All * (28 records)
Older than 30 days (0 records)
Older than six months (0 records)
Older than one year (0 records)
Note: A maximum number of 225000 log records can be deleted at once.
Make Backup
Backup List
Backup Scheduler
Endpoint Protector 4 Copyright 2004 - 2013 CoSoSys Ltd. All rights reserved.
Ready Version 4.4.0.1 - Appliance

Here you can select the logs you wish to backup. Simply select an option and click “Make Backup”.

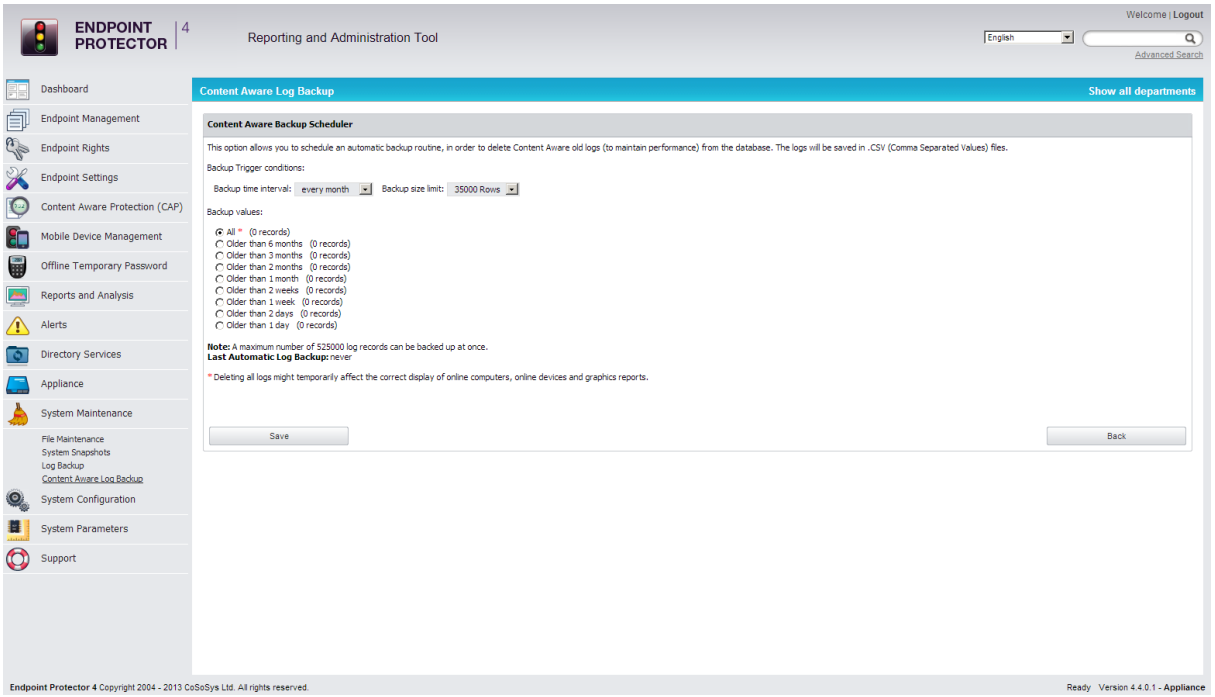


You should see the message “Backup Completed” in the top-center of your browser.

You can download and view the logs by selecting the “click here” link.

11.4.1. Automatic Scheduler (Automatic CAP Log Backup)

You can back up your log files also automatically by using the Backup Scheduler option.


ENDPOINT PROTECTOR 4
Reporting and Administration Tool
Welcome | Logout
English
Advanced Search
Dashboard
Endpoint Management
Endpoint Rights
Endpoint Settings
Content Aware Protection (CAP)
Mobile Device Management
Offline Temporary Password
Reports and Analysis
Alerts
Directory Services
Appliance
System Maintenance
File Maintenance
System Snapshots
Log Backup
Content Aware Log Backup
System Configuration
System Parameters
Support
Content Aware Log Backup
Show all departments
Content Aware Backup Scheduler
This option allows you to schedule an automatic backup routine, in order to delete Content Aware old logs (to maintain performance) from the database. The logs will be saved in .CSV (Comma Separated Values) files.
Backup Trigger conditions:
Backup time interval: every month
Backup size limit: 35000 Rows
Backup values:
All * (0 records)
Older than 6 months (0 records)
Older than 3 months (0 records)
Older than 2 months (0 records)
Older than 1 month (0 records)
Older than 2 weeks (0 records)
Older than 1 week (0 records)
Older than 2 days (0 records)
Older than 1 day (0 records)
Note: A maximum number of 525000 log records can be backed up at once.
Last Automatic Log Backup: never
* Deleting all logs might temporarily affect the correct display of online computers, online devices and graphics reports.
Save
Back
Endpoint Protector 4 Copyright 2004 - 2013 CoSoSys Ltd. All rights reserved.
Ready Version 4.4.0.1 - Appliance

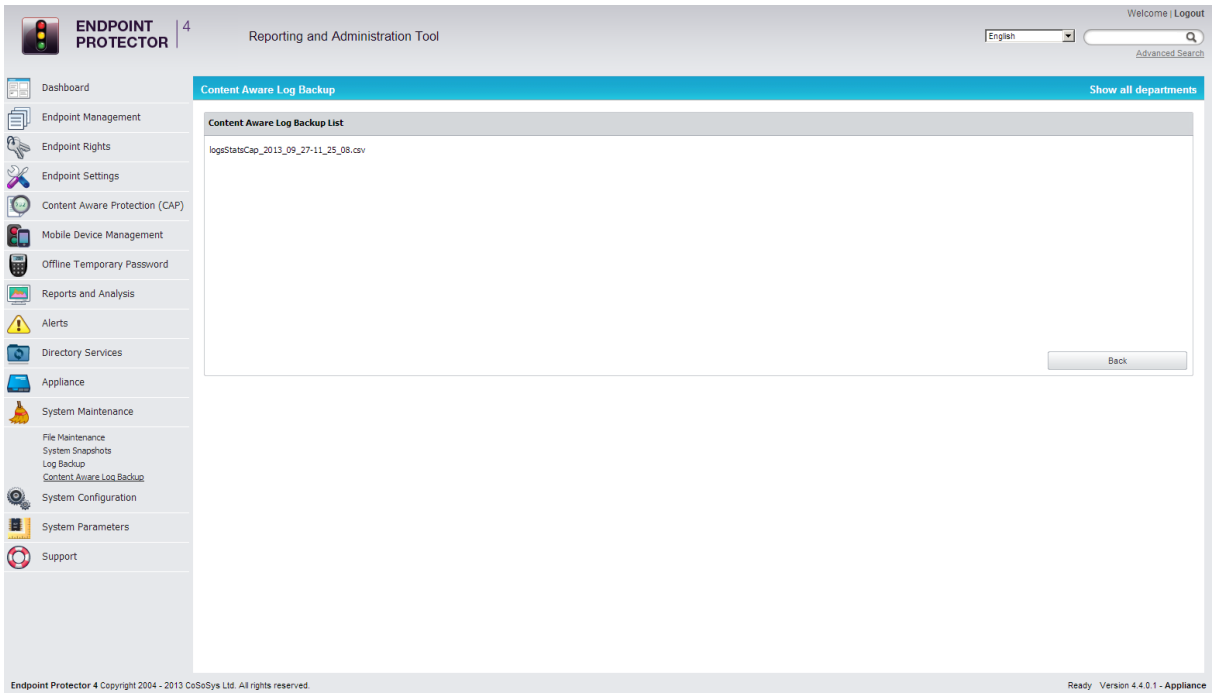
Here you can schedule an automatic backup routine by setting two trigger conditions:

Backup time interval - allows you to select a certain time interval for repeating the backup operation

Backup size limit - allows you to select a maximum size for the logs to be backed up

In case that you don't wish to set a specific value for one or both of these options, please leave the specific field(s) blank. After specifying the logs to be backed up automatically based on their creation time, please click "Save" in order for your options to be applied.

You can view the created backups by using the Backup List option.

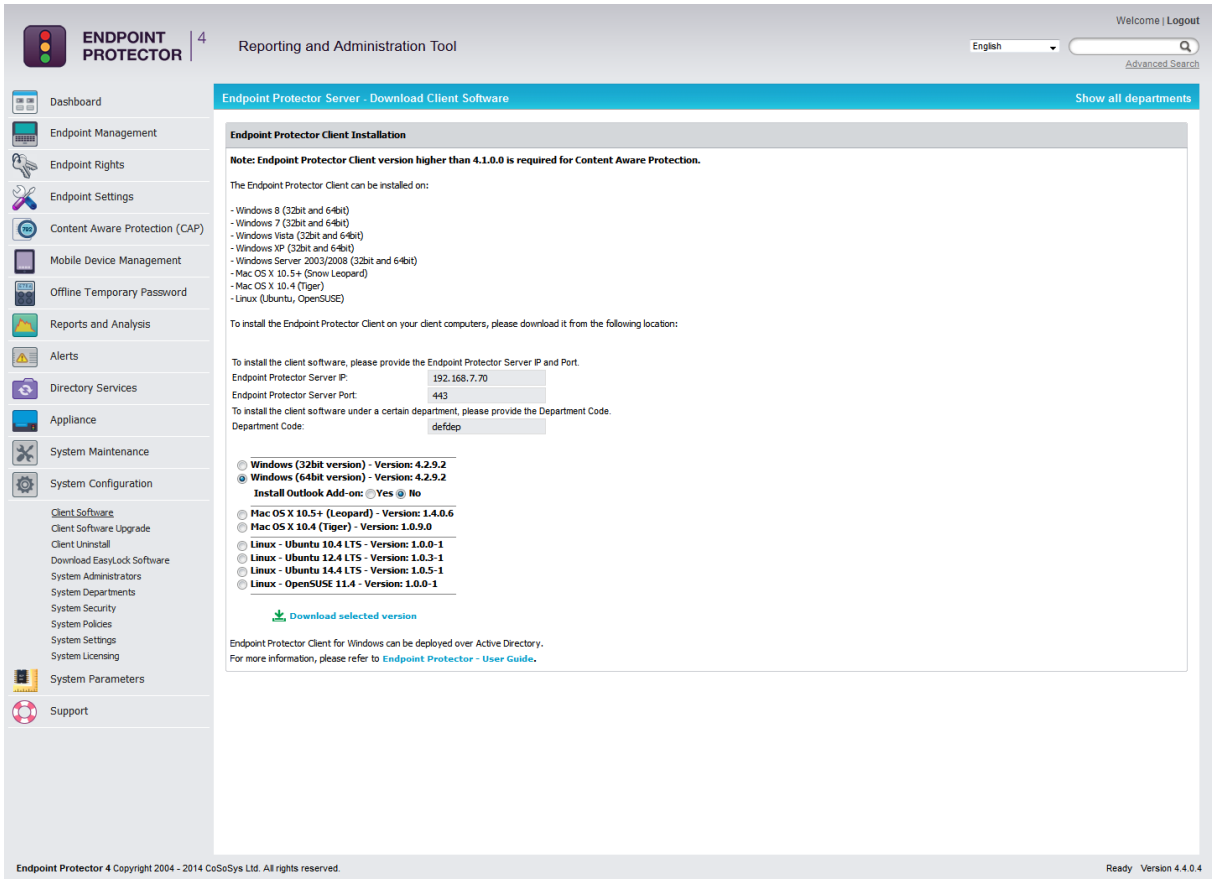


12. System Configuration

This module also contains advanced settings, which influence the functionality and stability of the system.

12.1. Client Software

In this section, the administrator can download and install the Endpoint Protector Client corresponding to the used operating system. Please note that our Server and Client are communicating through port 443.

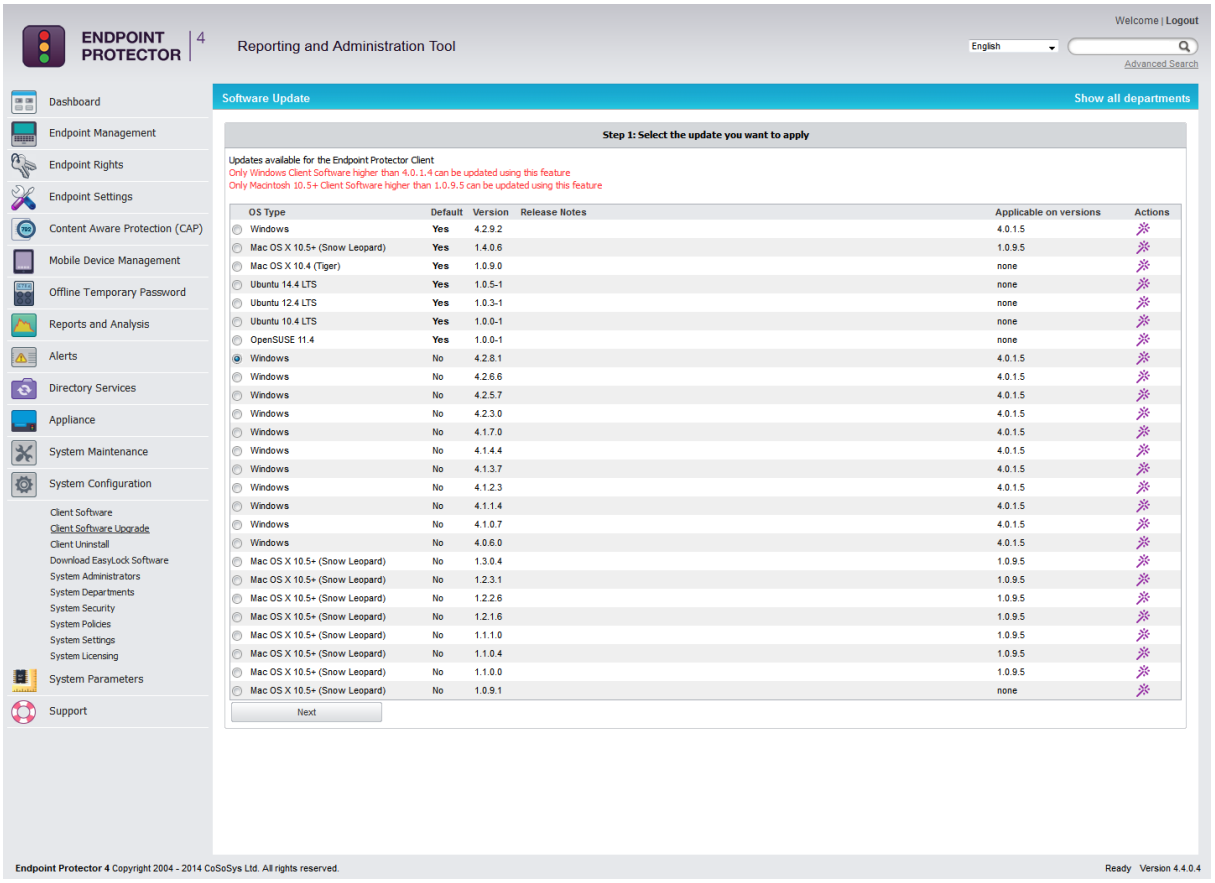

ENDPOINT PROTECTOR 4
Reporting and Administration Tool
Welcome | Logout
English
Advanced Search
Dashboard
Endpoint Management
Endpoint Rights
Endpoint Settings
Content Aware Protection (CAP)
Mobile Device Management
Offline Temporary Password
Reports and Analysis
Alerts
Directory Services
Appliance
System Maintenance
System Configuration
Client Software
Client Software Upgrade
Client Uninstall
Download EasyLock Software
System Administrators
System Departments
System Security
System Policies
System Settings
System Licensing
System Parameters
Support
Endpoint Protector Server - Download Client Software
Show all departments
Endpoint Protector Client Installation
Note: Endpoint Protector Client version higher than 4.1.0.0 is required for Content Aware Protection.
The Endpoint Protector Client can be installed on:
- Windows 8 (32bit and 64bit)
- Windows 7 (32bit and 64bit)
- Windows Vista (32bit and 64bit)
- Windows XP (32bit and 64bit)
- Windows Server 2003/2008 (32bit and 64bit)
- Mac OS X 10.5+ (Snow Leopard)
- Mac OS X 10.4 (Tiger)
- Linux (Ubuntu, OpenSUSE)
To install the Endpoint Protector Client on your client computers, please download it from the following location:
To install the client software, please provide the Endpoint Protector Server IP and Port.
Endpoint Protector Server IP: 192.168.7.70
Endpoint Protector Server Port: 443
To install the client software under a certain department, please provide the Department Code.
Department Code: defdep
Windows (32bit version) - Version: 4.2.9.2
Windows (64bit version) - Version: 4.2.9.2
Install Outlook Add-on: Yes No
Mac OS X 10.5+ (Leopard) - Version: 1.4.0.6
Mac OS X 10.4 (Tiger) - Version: 1.0.9.0
Linux - Ubuntu 10.4 LTS - Version: 1.0.0-1
Linux - Ubuntu 12.4 LTS - Version: 1.0.3-1
Linux - Ubuntu 14.4 LTS - Version: 1.0.5-1
Linux - OpenSUSE 11.4 - Version: 1.0.0-1
Download selected version
Endpoint Protector Client for Windows can be deployed over Active Directory.
For more information, please refer to Endpoint Protector - User Guide.
Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.
Ready Version 4.4.0.4

Note!

The Windows 32-bit and 64-bit client installers both offer the option to download the package with or without a Microsoft Outlook add-on. This option fixes any incompatibility that may arise between Microsoft Outlook and Endpoint Protector.

12.2. Client Software Upgrade

This section allows selecting and performing an automatic update of the installed Endpoint Protector Client version. Starting with Windows Client Version 4.2.3.0 a restart PC is mandatory in case of Client Software Upgrade is performed from Web UI.


ENDPOINT PROTECTOR 4
Reporting and Administration Tool
Welcome | Logout
English
Advanced Search
Dashboard
Endpoint Management
Endpoint Rights
Endpoint Settings
Content Aware Protection (CAP)
Mobile Device Management
Offline Temporary Password
Reports and Analysis
Alerts
Directory Services
Appliance
System Maintenance
System Configuration
Client Software
Client Software Upgrade
Client Uninstall
Download EasyLock Software
System Administrators
System Departments
System Security
System Policies
System Settings
System Licensing
System Parameters
Support
Software Update
Show all departments
Step 1: Select the update you want to apply
Updates available for the Endpoint Protector Client
Only Windows Client Software higher than 4.0.1.4 can be updated using this feature
Only Macintosh 10.5+ Client Software higher than 1.0.9.5 can be updated using this feature
OS Type | Default | Version | Release Notes | Applicable on versions | Actions
Windows | Yes | 4.2.9.2 | 4.0.1.5
Mac OS X 10.5+ (Snow Leopard) | Yes | 1.4.0.6 | 1.0.9.5
Mac OS X 10.4 (Tiger) | Yes | 1.0.9.0 | none
Ubuntu 14.4 LTS | Yes | 1.0.5-1 | none
Ubuntu 12.4 LTS | Yes | 1.0.3-1 | none
Ubuntu 10.4 LTS | Yes | 1.0.0-1 | none
OpenSUSE 11.4 | Yes | 1.0.0-1 | none
Windows | No | 4.2.8.1 | 4.0.1.5
Windows | No | 4.2.6.6 | 4.0.1.5
Windows | No | 4.2.5.7 | 4.0.1.5
Windows | No | 4.2.3.0 | 4.0.1.5
Windows | No | 4.1.7.0 | 4.0.1.5
Windows | No | 4.1.4.4 | 4.0.1.5
Windows | No | 4.1.3.7 | 4.0.1.5
Windows | No | 4.1.2.3 | 4.0.1.5
Windows | No | 4.1.1.4 | 4.0.1.5
Windows | No | 4.1.0.7 | 4.0.1.5
Windows | No | 4.0.6.0 | 4.0.1.5
Mac OS X 10.5+ (Snow Leopard) | No | 1.3.0.4 | 1.0.9.5
Mac OS X 10.5+ (Snow Leopard) | No | 1.2.3.1 | 1.0.9.5
Mac OS X 10.5+ (Snow Leopard) | No | 1.2.2.6 | 1.0.9.5
Mac OS X 10.5+ (Snow Leopard) | No | 1.2.1.6 | 1.0.9.5
Mac OS X 10.5+ (Snow Leopard) | No | 1.1.1.0 | 1.0.9.5
Mac OS X 10.5+ (Snow Leopard) | No | 1.1.0.4 | 1.0.9.5
Mac OS X 10.5+ (Snow Leopard) | No | 1.1.0.0 | 1.0.9.5
Mac OS X 10.5+ (Snow Leopard) | No | 1.0.9.1 | none
Next
Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.
Ready Version 4.4.0.4

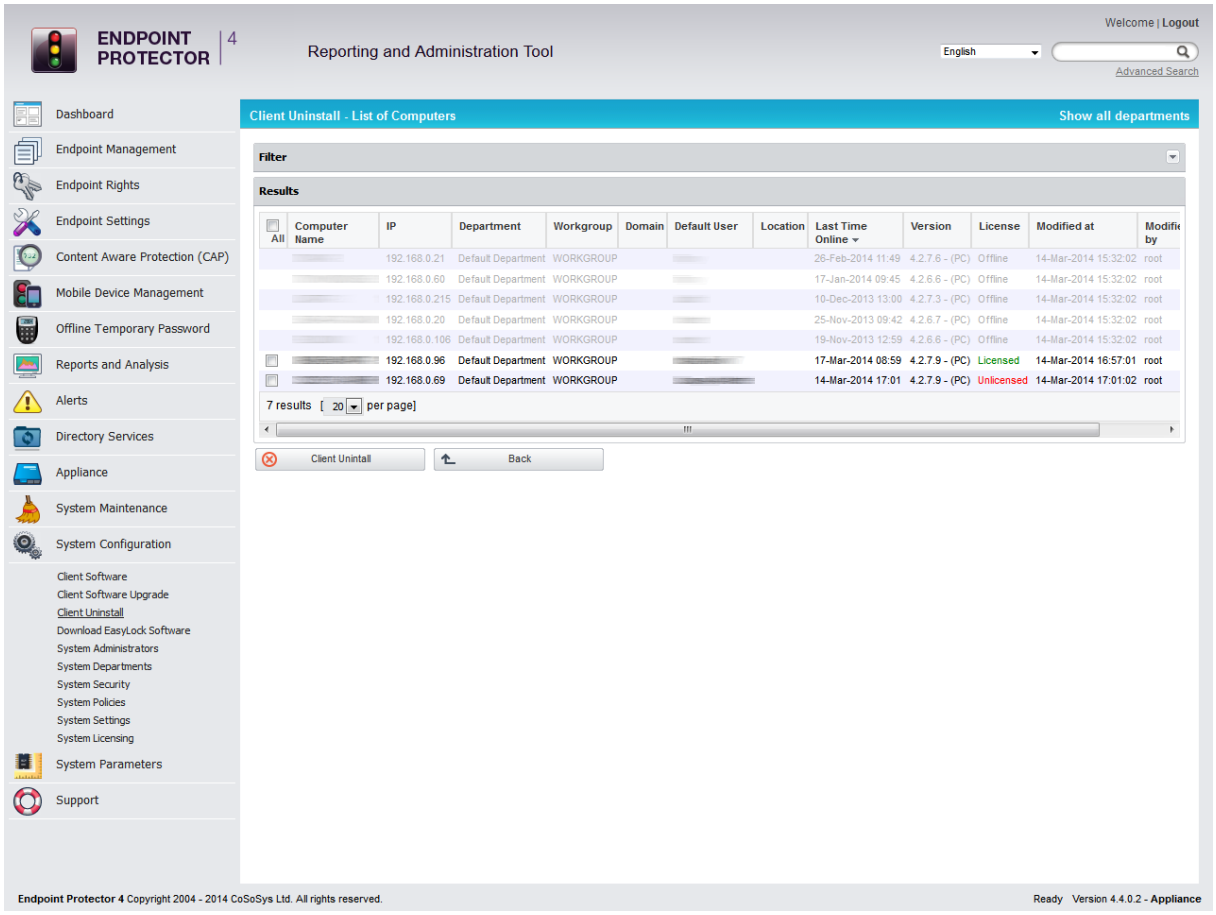
The button under the Actions column allows setting the default Endpoint Protector Client version that will be available for download under the Client Software section.

Note!

Downgrading from a currently installed Endpoint Protector Client version to an older one cannot be performed automatically.

12.3. Client Uninstall

The EPP Clients installed on the computers can be remotely uninstalled from this tab. The computers will receive the uninstall command at the same time they receive the next set of commands from the server. If the computer is offline it will receive the uninstall command the first time it will come online. When the uninstall button is pressed the computer(s) will be greyed out until the action will be performed. The uninstall command can be cancelled if it was not already executed.

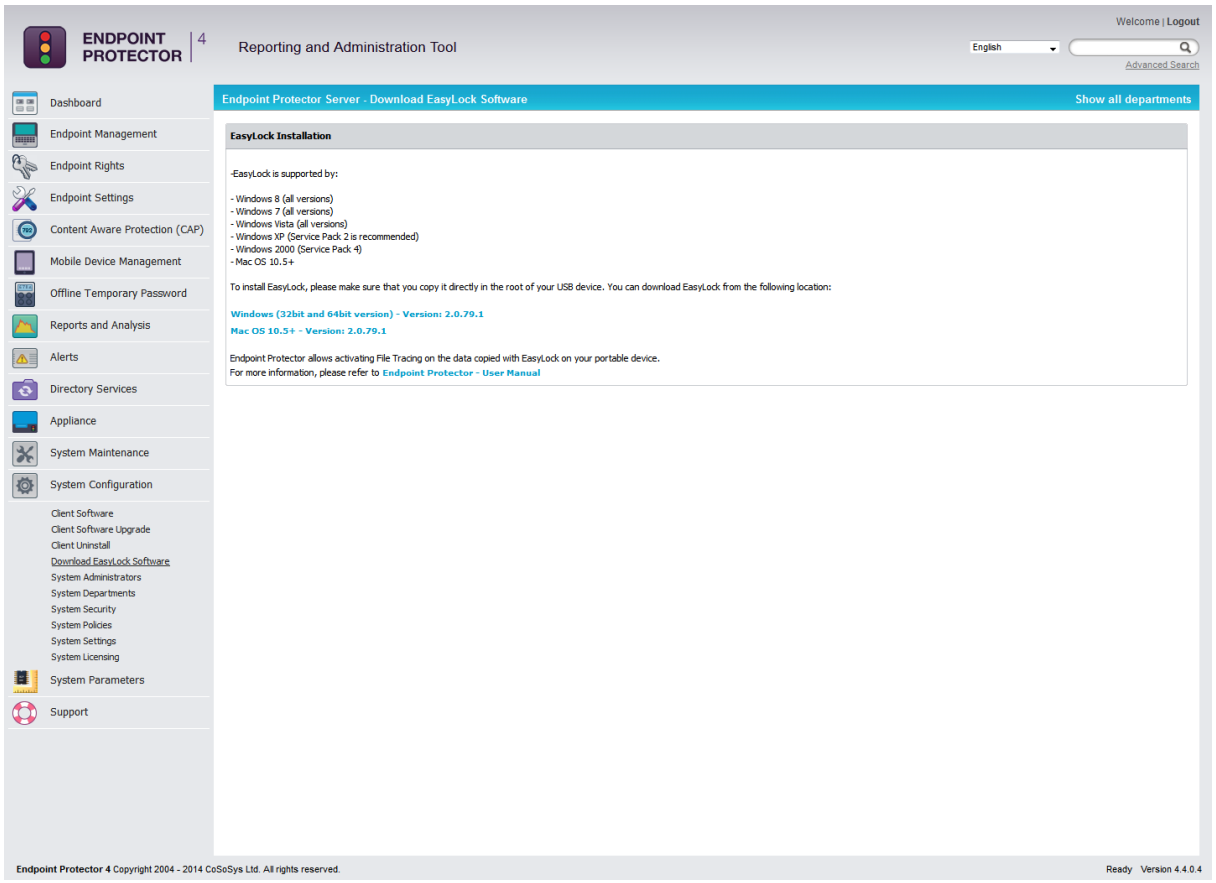


Note!

The uninstall command works for Windows client version 4.2.8.1 or newer.

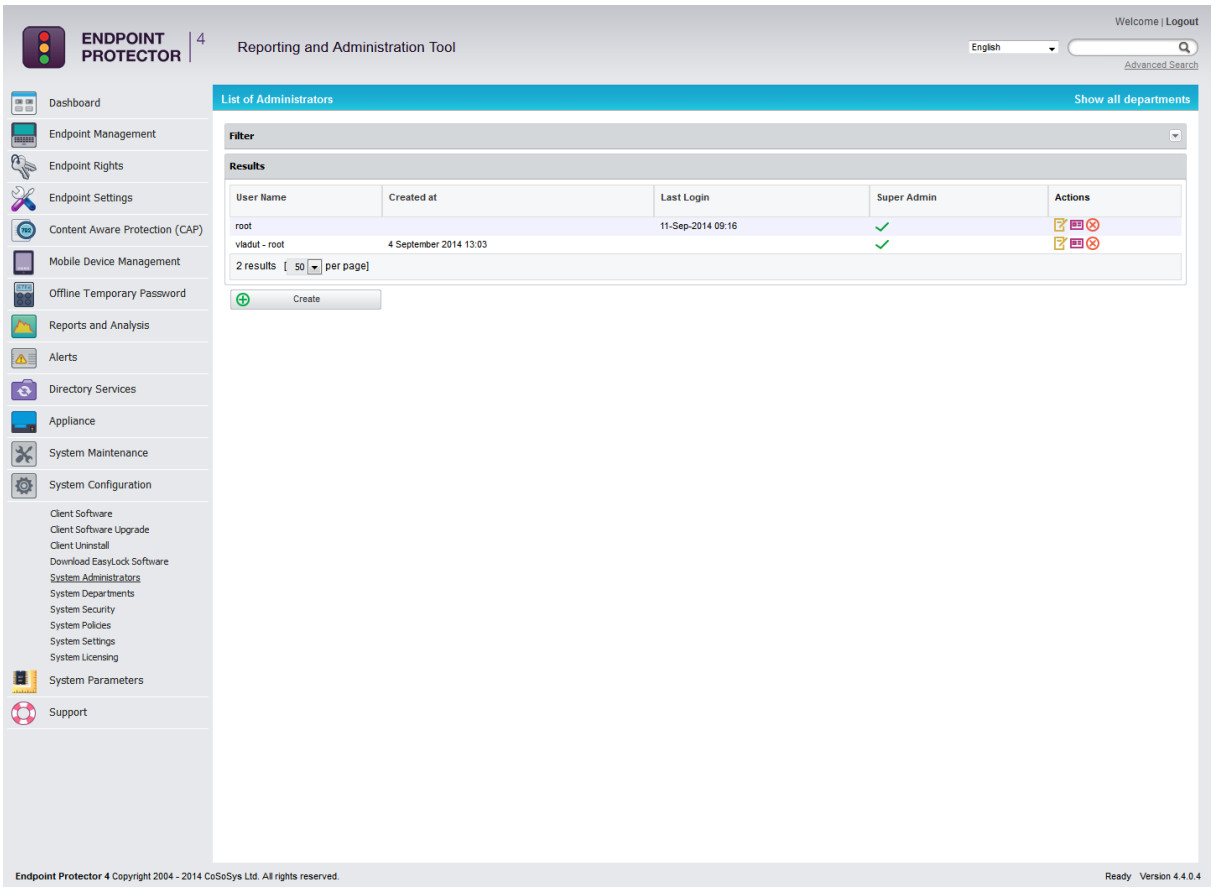
12.4. EasyLock Software Download

The EasyLock software can be downloaded directly from this section and copied to the root folder of the selected USB Drive. It supports computers running on both Windows and Mac OS X 10.5+.


ENDPOINT PROTECTOR 4
Reporting and Administration Tool
Welcome | Logout
English
Advanced Search
Dashboard
Endpoint Management
Endpoint Rights
Endpoint Settings
Content Aware Protection (CAP)
Mobile Device Management
Offline Temporary Password
Reports and Analysis
Alerts
Directory Services
Appliance
System Maintenance
System Configuration
Client Software
Client Software Upgrade
Client Uninstall
Download EasyLock Software
System Administrators
System Departments
System Security
System Policies
System Settings
System Licensing
System Parameters
Support
Endpoint Protector Server - Download EasyLock Software
Show all departments
EasyLock Installation
-EasyLock is supported by:
- Windows 8 (all versions)
- Windows 7 (all versions)
- Windows Vista (all versions)
- Windows XP (Service Pack 2 is recommended)
- Windows 2000 (Service Pack 4)
- Mac OS 10.5+
To install EasyLock, please make sure that you copy it directly in the root of your USB device. You can download EasyLock from the following location:
Windows (32bit and 64bit version) - Version: 2.0.79.1
Mac OS 10.5+ - Version: 2.0.79.1
Endpoint Protector allows activating File Tracing on the data copied with EasyLock on your portable device.
For more information, please refer to Endpoint Protector - User Manual
Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.
Ready Version 4.4.0.4

12.5. System Administrators

This list contains all the administrators who have access to the Administration and Reporting Tool. As described earlier in this document, the administrators can be: regular administrators, which have some limitations and super administrators which have full access to the system, including advanced features.

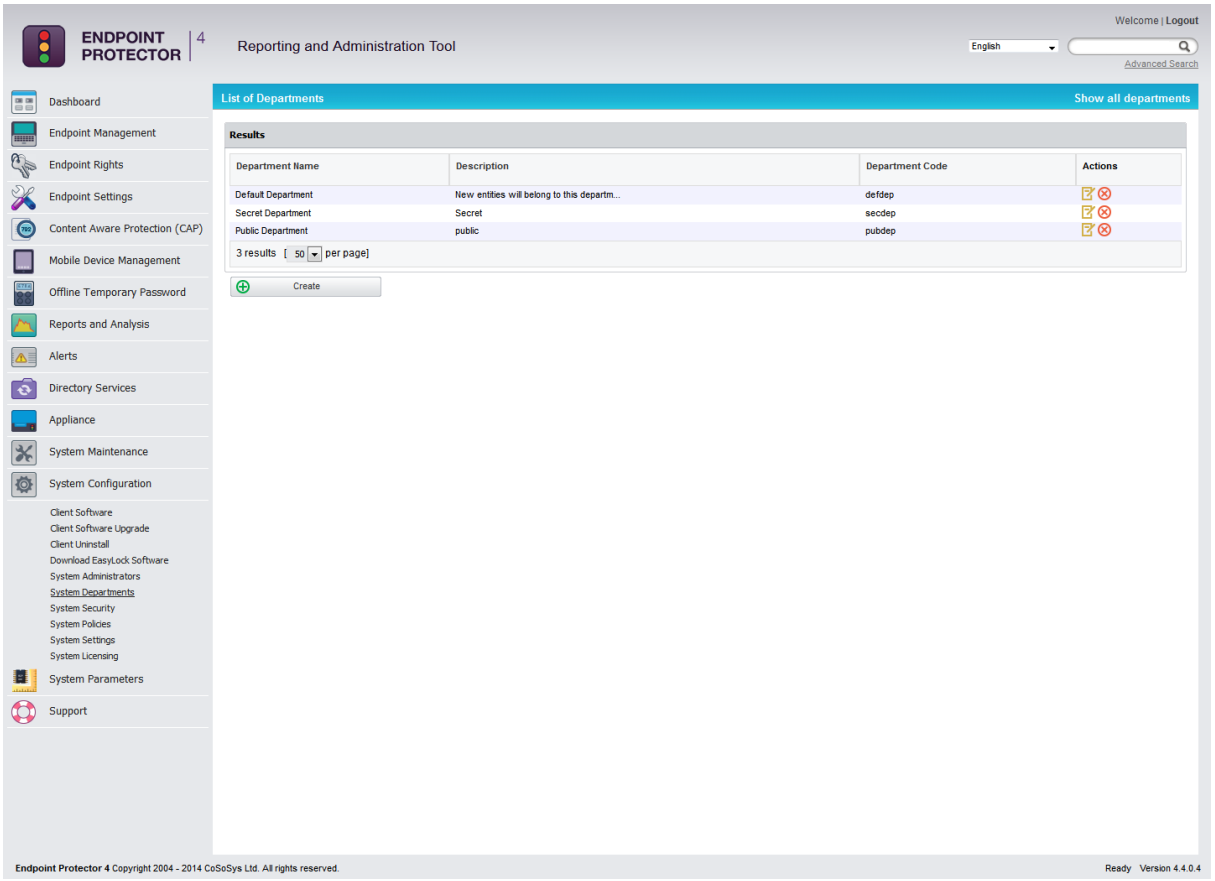


For more information on administrators, please see paragraph 12.1 “Adding new administrator(s)”.

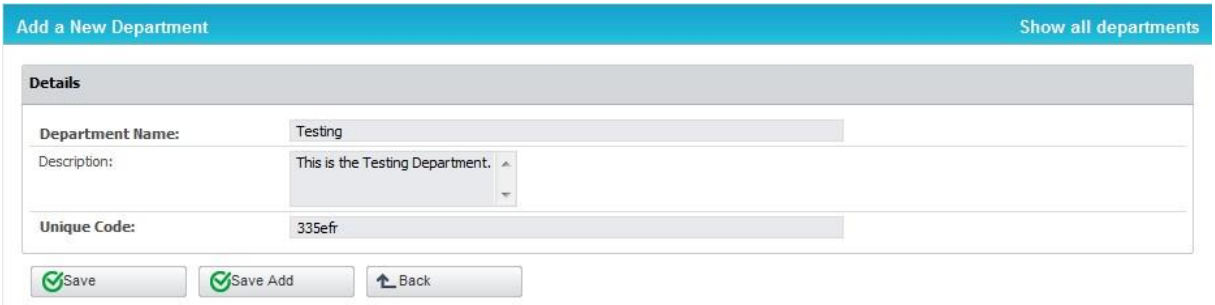
12.6. System Departments

This module allows creating System Departments. The available options are **Edit** and **Delete**.

The main reason for using this feature is to target Large Installation where one Super Administrator cannot handle the Endpoint Protector Server configuration and maintenance. Even further, one Regular administrator should only be responsible for his entities.



A new department can be defined by using the “Create” button.



Even if the term Department is simple, if we want to make a similarity between Endpoint Protector and Active Directory (or any other Director Service software) the equivalent of this term is Organization Unit. Of course Organization Unit is not identical with Department, and again Endpoint Protector leaves the power to the actual Super Administrator to virtually link one or more Organization Units to an Endpoint Protector Department. For more details, please see paragraph "10.1. AD Deployment".

Several aspects regarding departments are detailed below:

1. Each main entity must belong to a department, except with the scenario when the super administrator deletes the Default Department. At computer registration, the Department Code is provided. If a department having the given code is found, then the computer will register and it will belong to that department. All the main entities information received from a computer in department X will also belong to department X.

Example: Computer Test-PC is registered to department "developers". In this case, user Test logged on that computer will be assigned to the same department together with the devices connected on the computer Test-PC.

Note!

In case that, at registration, no department code is provided or a wrong department code is provided, the department code is considered invalid and that computer will be assigned to the default department (defdep).

2. Super Administrators (example root) will still have access to all the main entities regardless of their departments and will be able to change departments. When logged on as Super Administrator, the text "Show all departments" will be displayed on the right top part of the main content layout of the Web interface.

3. As only the Super Administrator has the possibility to create regular users, he is also responsible for assigning regular administrators to handle one or more departments. Regular Administrator will see and manage in the Web interface only the main entities belonging to the assigned departments.

4. From a security stand point of view:

A Regular Administrator should only see his department's entities and nothing more.

A Regular Administrator should only control his department's entities and nothing more.

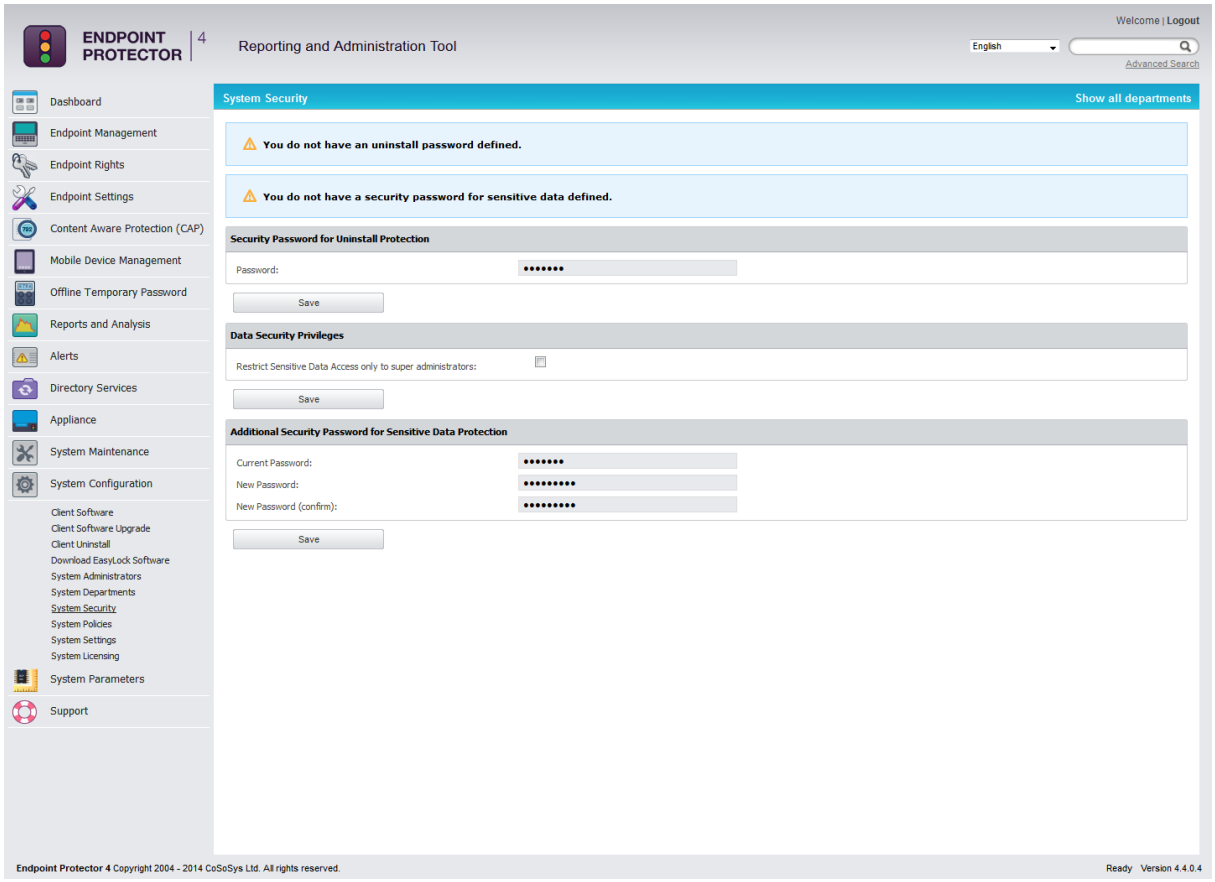
IMPORTANT!

If you do not want to have any departments based organization within the Endpoint Protector deployment, please make sure that you always assign the default Department to all new created Regular Administrators within the Endpoint Protector Web Interface.

12.7. System Security / Client Uninstall Protection

The Client Uninstall Protection feature protects the Endpoint Protector Client from being uninstalled by using a password-based mechanism. The Administrator of the system defines this password from within the Reporting and Administration Tool of Endpoint Protector 4. When somebody tries to uninstall the Endpoint Protector Client, they will be prompted for the password. If they do not know the password, the Client removal cannot continue.

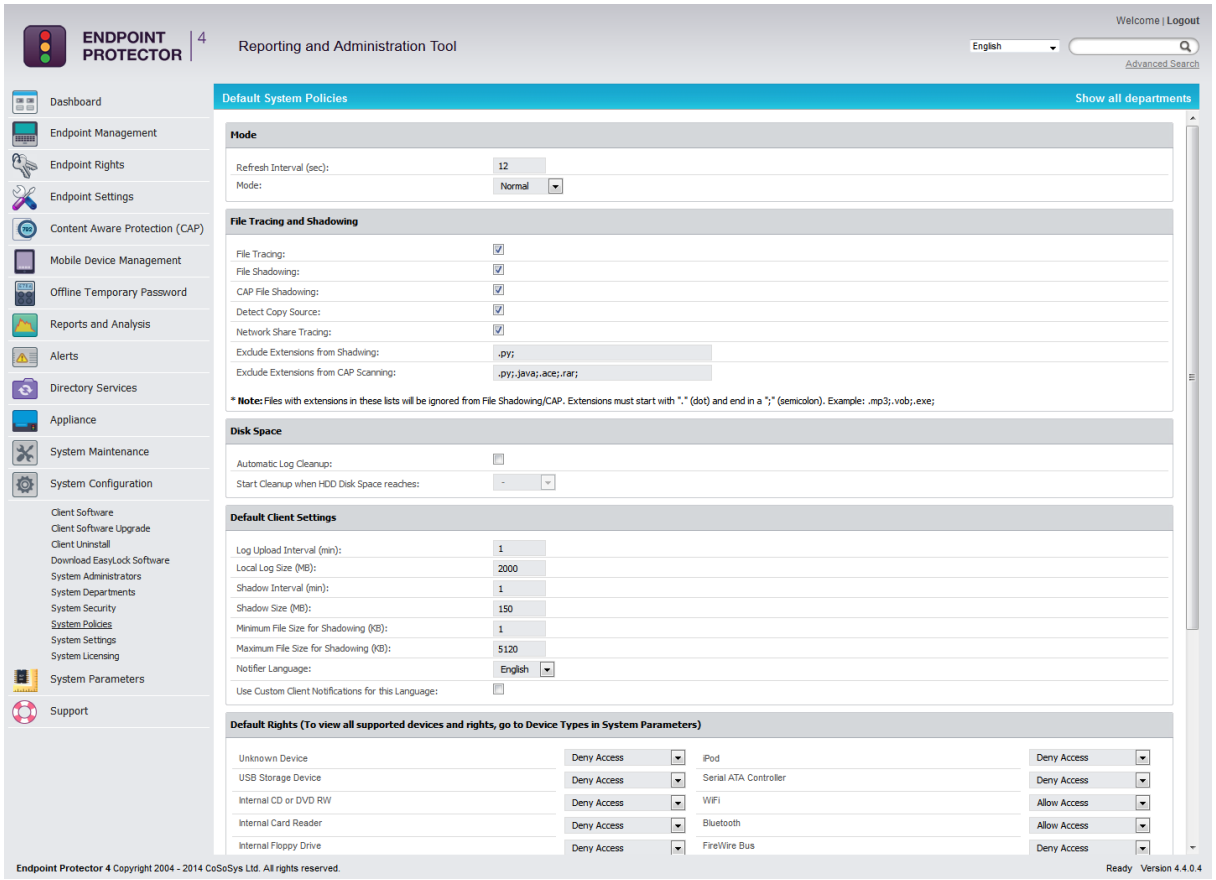
This password can be set by accessing "System Configuration" – "System Security", entering a password in the "Password" field and clicking on "Save".



The second option, "**Data Security Privileges**", allows you to restrict Sensitive Data sections access only to Super Administrators. If this option is selected, then only super administrators are able to view the "Reports and Analysis" section. If this option is not selected, then super administrators and also administrators are able to view the "Reports and Analysis" section.

12.8. System Policies

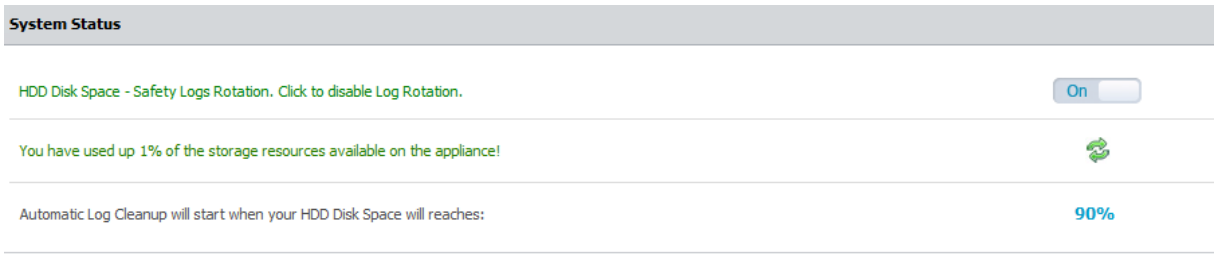
This module provides a useful shortcut to default server and device rights settings. By accessing this module you can quickly and easily configure the Endpoint Protector 4 Server settings such as Log Upload Interval (in minutes), Local Shadow Size (in MB), Local Log Size (in KB), etc. and default device group behavior, for each device type, separately. There is also an option to manage the server's disk space. The Administrator can enable a functionality called "Automatic Log Cleanup". Once enabled by click System Policies -> Automatic Disk Cleanup, the server will start to overwrite old logs when it reaches a predefined percent value. By doing this, the server will never reach a hard drive space limit.



To store your setup, simply click "Save".

Note!

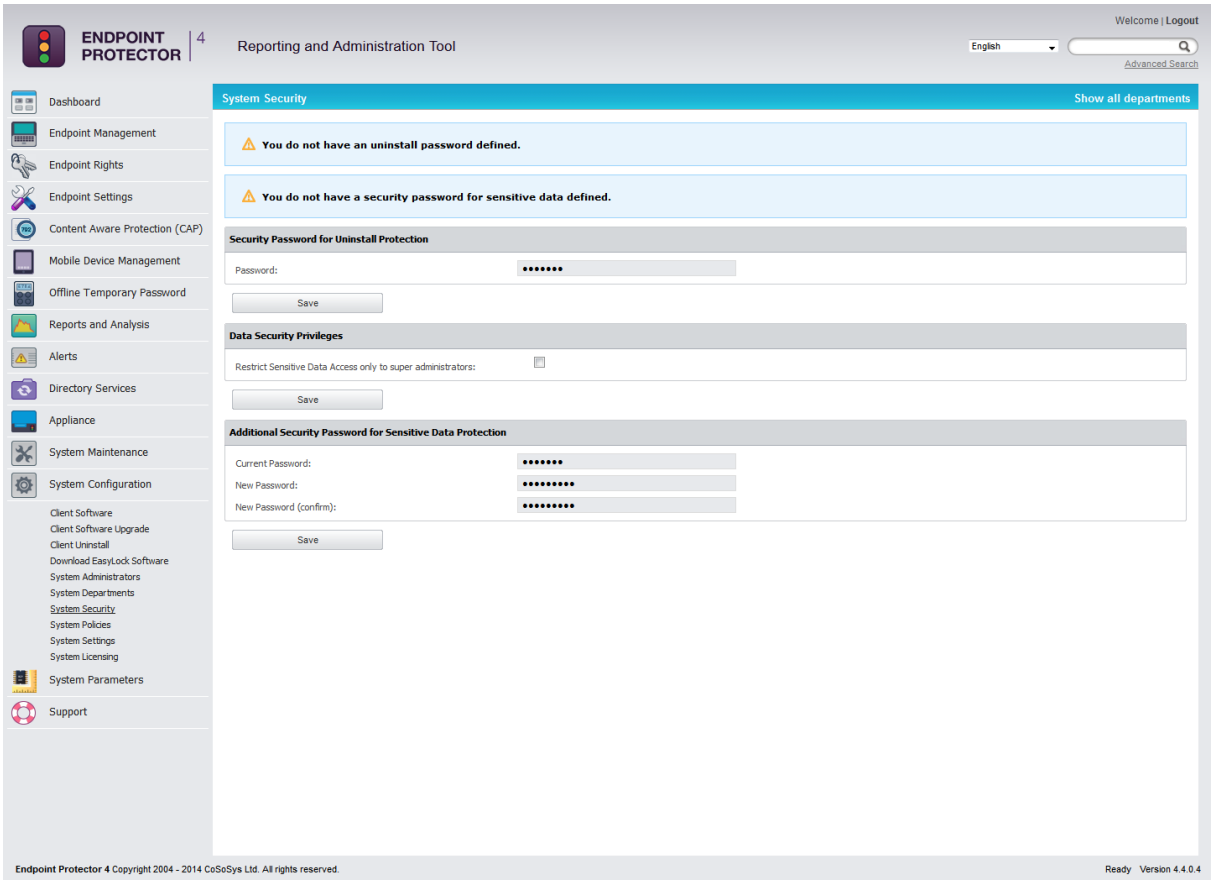
The “Automatic Log Cleanup” option can also be activated from the Dashboard -> System Status


System Status
HDD Disk Space - Safety Logs Rotation. Click to disable Log Rotation.
On
You have used up 1% of the storage resources available on the appliance!
Automatic Log Cleanup will start when your HDD Disk Space will reaches:
90%

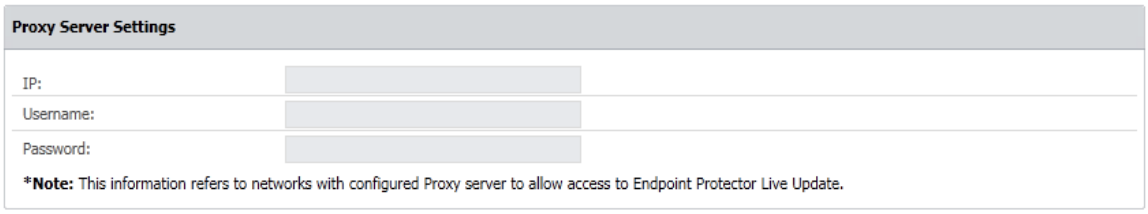
12.9. System Settings

In the System Settings module, you can modify Endpoint Protector 4 Server Rights functionalities by giving priority to either User Rights or Computer Rights.

Pease see the "Setting up policies" chapter of this document for more information on this area.



Endpoint Protector 4 offers a new configuration option: **Proxy Settings**.


Proxy Server Settings
IP:
Username:
Password:
*Note: This information refers to networks with configured Proxy server to allow access to Endpoint Protector Live Update.

Due to the increasing number of companies that have a Proxy server in their network to control external access, it appeared the need to provide a way of configuring this information also in Endpoint Protector.

The necessary configuration details are:

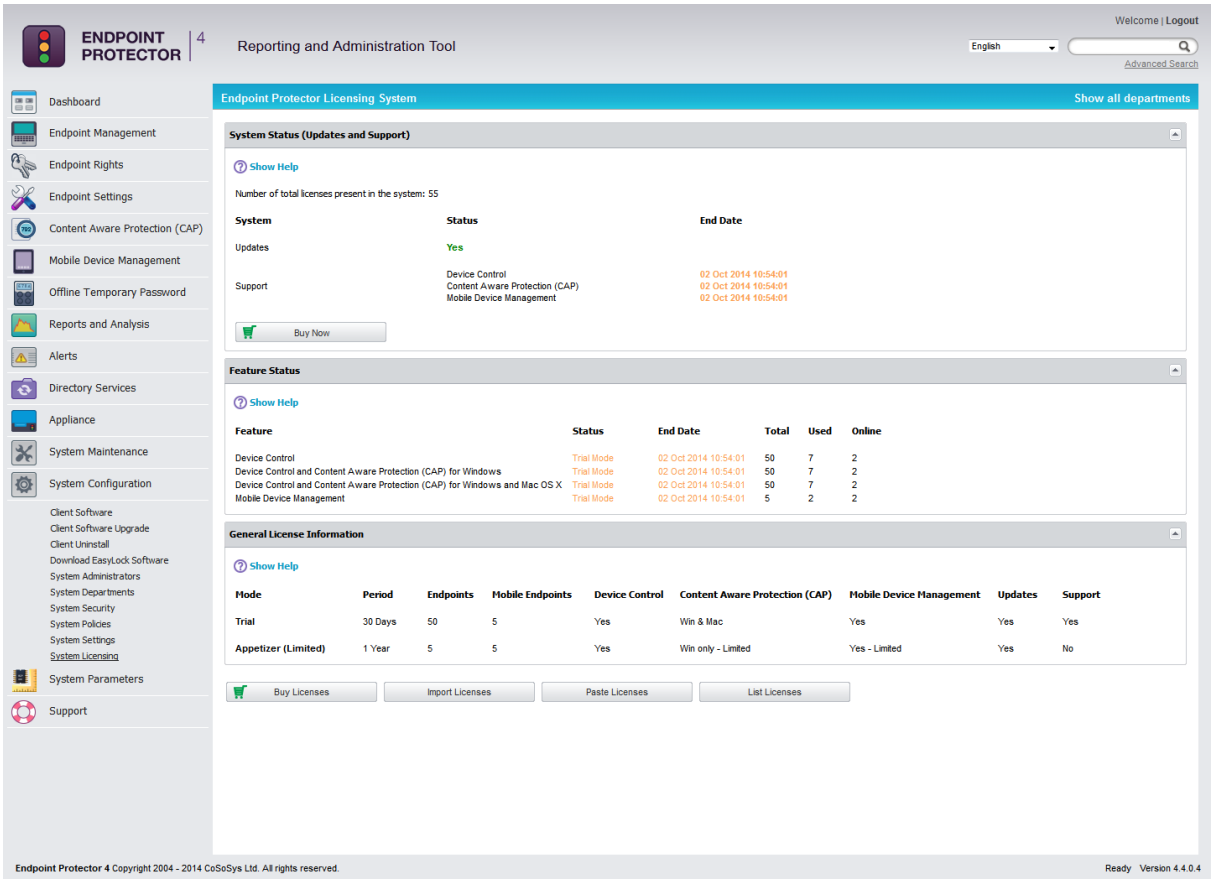
- IP – the Proxy Server IP
- Username/Password – Proxy access credentials (not mandatory)

Attention!

If these details are not filled in, Endpoint Protector will connect directly to liveupdate.endpointprotector.com. Data sent to this server is not security sensitive, being limited only to your version/language.

12.10. System Licensing

This module allows the administrator to manage the licensing of Endpoint Protector and offers a complete overview of the current licenses status.



The Endpoint Protector licensing system comprises three types of licenses: Endpoint licenses for Mobile and Fixed endpoints, Feature licenses and Updates & Support licenses.

Endpoint licenses are used for registering the Endpoint Protector Client, enabling the communication with the Endpoint Protector Server. They are available as either 30 days Trial licenses or perpetual (permanent) licenses. Once registered with a valid Endpoint license, the Endpoint Protector Client remains

active for an unlimited period of time regardless of the status of the other license types.

Feature licenses are used for activating one of the three Endpoint Protector modules: Device Control, Content Aware Protection, respectively Mobile Device Management. Each of these modules can be used in Trial Mode for a period of up to 30 days. Then, a perpetual (permanent) license is required to be purchased and imported for the feature to remain active. Although the Device Control module appears by default as active in the Web Administration Interface, a license is required to enable the communication between Server and Client. The Content Aware Protection and Mobile Device Management features are displayed as blocked by default and require an additional Activation request to be performed by the administrator. The Features Status section offers an overview of the current features licensing status.

Updates & Support licenses are optional licenses that once purchased and imported into the system allow access to the latest Updates available for both Client and Server side and enable premium Support and Technical Assistance. The Updates and Support licenses can be purchased for a period varying from 1 month up to 36 months, with a separate option for 120 months. As opposed to Endpoint and Feature licenses, Updates & Support licenses are not permanent and they require periodic renewal for being able to get access to our Live Update Server.

Note!

When first activating one or more features, an Updates & Support license for a period of minimum 1 year is required. After the Updates & Support license expires, the feature remains active and purchasing additional Updates & Support licenses becomes optional.

For example, if you wish to license Endpoint Protector for 100 workstations and use the Content Aware Protection module for 1 year, you will require:

- 100 Endpoint licenses
- 1 Content Aware Protection license, which includes an Updates & Support license for Device Control and Content Aware Protection valid for 1 year. After the validity period expires, the feature remains active, while any updates and support services are not available anymore.

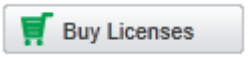
If you wish to manage also a fleet of 10 devices for 6 months, you will additionally require:

- 10 Mobile Endpoint licenses
- 1 Mobile Device Management license, which includes an Updates & Support license for Mobile Device Management for 6 months

Note!

As opposed to Device Control and Content Aware Protection, a valid Updates & Support license for Mobile Device Management is required for the feature to remain active as the Mobile Device Management service requires a working connection to our Cloud.

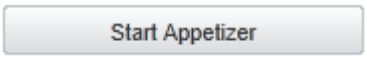
All license types can be purchased directly by using the "Buy Licenses" option.



A separate free licensing option, called **Appetizer Mode**, is available for small networks of up to 5 computers and / or 5 iOS and Android devices. Appetizer licenses enable access to each of the three Endpoint Protector modules for a period of 1 year.

12.10.1. Appetizer Mode

The Appetizer Mode can be activated by pushing the "Start Appetizer" button, which will automatically assign 1 year Device Control and Content Aware Protection licenses for up 5 computers. Additionally, it will enable a 1 year subscription for Mobile Device Management by Endpoint Protector for up to 5 iOS and Android smartphones and tablets.



The Appetizer license is a limited license valid for 1 year with automatic renewal, which includes also 1 year of updates with automatic renewal. The following limitations apply:

- **No Support Included!**
- **Device Control**: no limitations
- **Content Aware Protection**: The options for E-mail, Web Browsers and Cloud Services/File Sharing, Clipboard Monitor and Print Screen Monitor are disabled. Mac OS X compatibility is also disabled.
- **Mobile Device Management**: mobile device tracking is disabled.

Note!

License terms may change without prior notice.

Several Requirements are necessary for using Appetizer Licenses:

- Licensee has to be small business or registered professional (e.g. a company such as a Ltd. or a registered professional such as a law firm or architectural association).
- Valid company e-mail address
- Online activation of virtual appliance after setup in your network
- Online self-enrollment of MDM services (e.g. for Apple Push Notification Certificate)

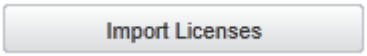
12.10.2. Trial Mode

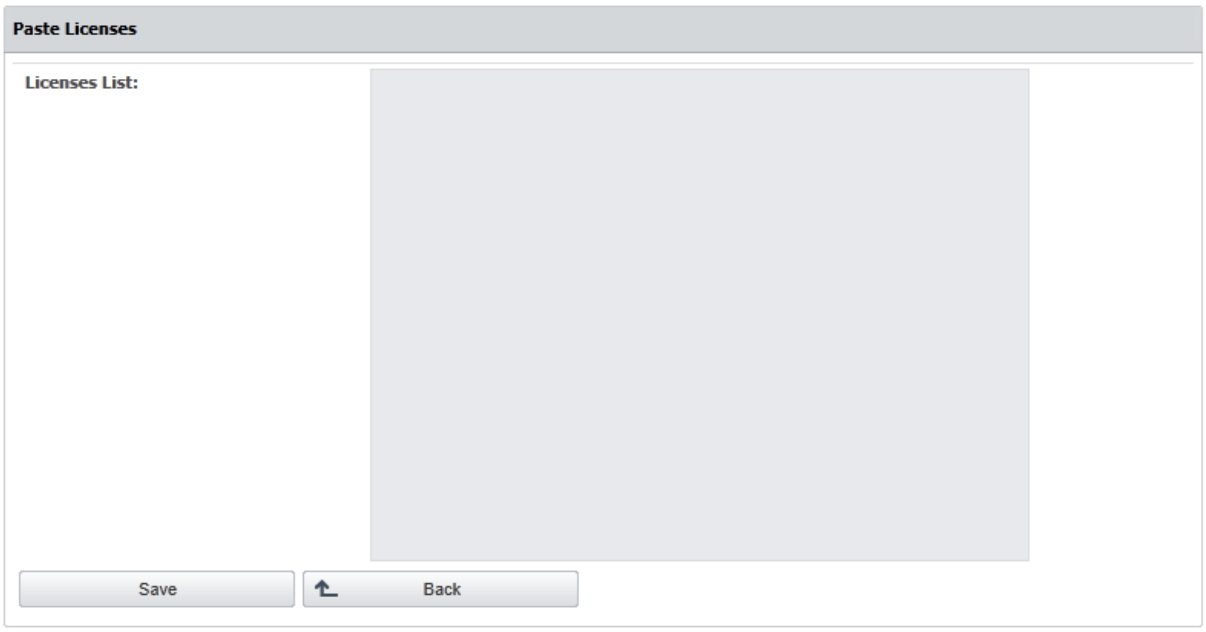
The trial period can be activated by pushing the "Start Free Trial" button, which will automatically assign 30 days trial licenses for up to 50 computers.

The trial licenses are assigned on a "first-in-first-served" basis. In case that one or more computers with assigned trial licenses are inactive for a certain interval of time, the administrator can manually release those licenses, which will automatically be reassigned to other online computers.

12.10.3. Import Licenses

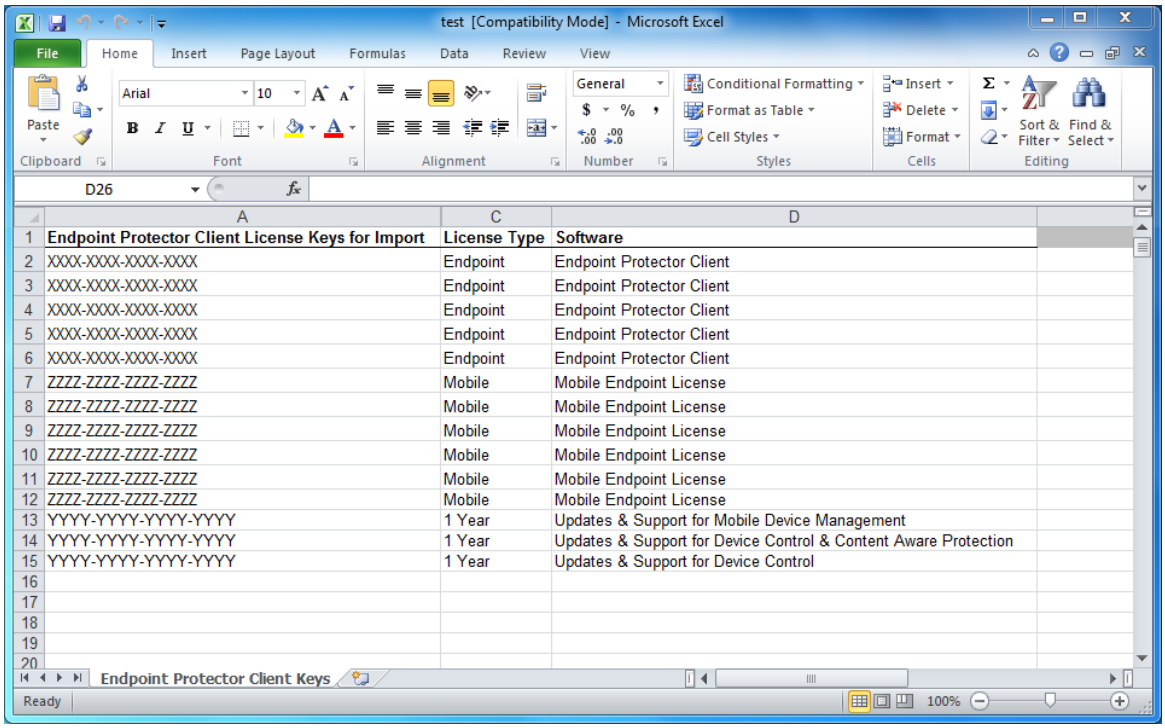
The Import Licenses option gives you the possibility to browse for an Excel file that contains licenses. After you have selected the file, click Upload.





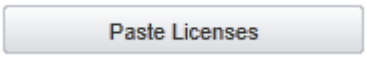
Attention!

The Excel document has to be formatted in a specific way. Only the first column in the excel sheet is taken into consideration and the first line in the excel sheet is ignored.

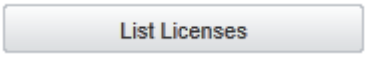


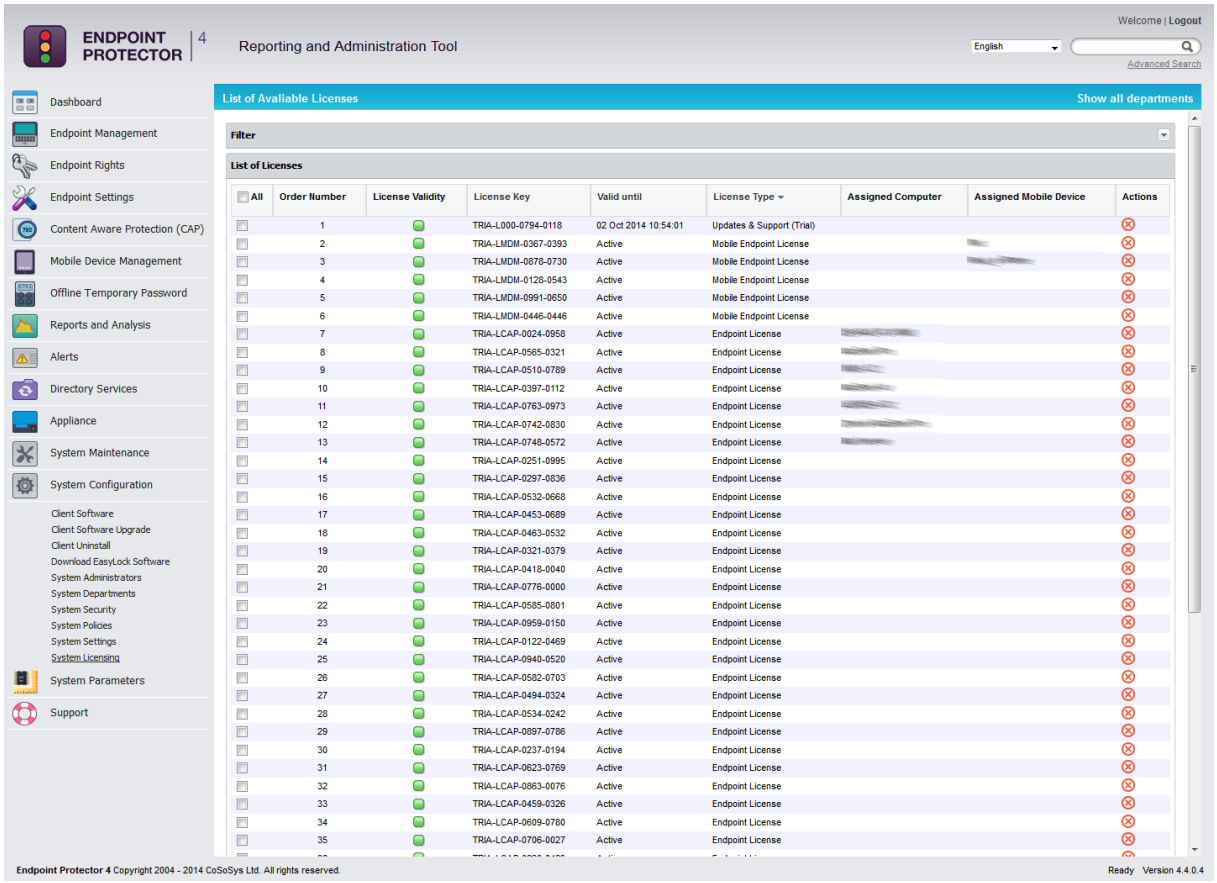
	A	C	D
1	Endpoint Protector Client License Keys for Import	License Type	Software
2	XXXX-XXXX-XXXX-XXXX	Endpoint	Endpoint Protector Client
3	XXXX-XXXX-XXXX-XXXX	Endpoint	Endpoint Protector Client
4	XXXX-XXXX-XXXX-XXXX	Endpoint	Endpoint Protector Client
5	XXXX-XXXX-XXXX-XXXX	Endpoint	Endpoint Protector Client
6	XXXX-XXXX-XXXX-XXXX	Endpoint	Endpoint Protector Client
7	ZZZZ-ZZZZ-ZZZZ-ZZZZ	Mobile	Mobile Endpoint License
8	ZZZZ-ZZZZ-ZZZZ-ZZZZ	Mobile	Mobile Endpoint License
9	ZZZZ-ZZZZ-ZZZZ-ZZZZ	Mobile	Mobile Endpoint License
10	ZZZZ-ZZZZ-ZZZZ-ZZZZ	Mobile	Mobile Endpoint License
11	ZZZZ-ZZZZ-ZZZZ-ZZZZ	Mobile	Mobile Endpoint License
12	ZZZZ-ZZZZ-ZZZZ-ZZZZ	Mobile	Mobile Endpoint License
13	YYYY-YYYY-YYYY-YYYY	1 Year	Updates & Support for Mobile Device Management
14	YYYY-YYYY-YYYY-YYYY	1 Year	Updates & Support for Device Control & Content Aware Protection
15	YYYY-YYYY-YYYY-YYYY	1 Year	Updates & Support for Device Control
16			
17			
18			
19			
20			

Licenses can be imported also by using the “Paste Licenses” option, which allows to manually copy&paste licenses into the system. This option is recommended for online purchases, when licenses are delivered directly in your e-mail.



The List Licenses button displays the list of imported license keys, including the computers to which they were asisgned and the validity period.




ENDPOINT PROTECTOR 4
Reporting and Administration Tool
Welcome | Logout
English
Advanced Search
Dashboard
Endpoint Management
Endpoint Rights
Endpoint Settings
Content Aware Protection (CAP)
Mobile Device Management
Offline Temporary Password
Reports and Analysis
Alerts
Directory Services
Appliance
System Maintenance
System Configuration
Client Software
Client Software Upgrade
Client Uninstall
Download EasyLock Software
System Administrators
System Departments
System Security
System Policies
System Settings
System Licensing
System Parameters
Support
List of Avaliable Licenses
Show all departments
Filter
List of Licenses
All
Order Number
License Validity
License Key
Valid until
License Type
Assigned Computer
Assigned Mobile Device
Actions
1 TRIA-L000-0794-0118 02 Oct 2014 10:54:01 Updates & Support (Trial)
2 TRIA-LMDM-0367-0393 Active Mobile Endpoint License
3 TRIA-LMDM-0878-0730 Active Mobile Endpoint License
4 TRIA-LMDM-0128-0543 Active Mobile Endpoint License
5 TRIA-LMDM-0991-0650 Active Mobile Endpoint License
6 TRIA-LMDM-0446-0446 Active Mobile Endpoint License
7 TRIA-LCAP-0024-0958 Active Endpoint License
8 TRIA-LCAP-0565-0321 Active Endpoint License
9 TRIA-LCAP-0510-0789 Active Endpoint License
10 TRIA-LCAP-0397-0112 Active Endpoint License
11 TRIA-LCAP-0763-0973 Active Endpoint License
12 TRIA-LCAP-0742-0830 Active Endpoint License
13 TRIA-LCAP-0748-0572 Active Endpoint License
14 TRIA-LCAP-0251-0995 Active Endpoint License
15 TRIA-LCAP-0297-0836 Active Endpoint License
16 TRIA-LCAP-0532-0668 Active Endpoint License
17 TRIA-LCAP-0453-0689 Active Endpoint License
18 TRIA-LCAP-0463-0532 Active Endpoint License
19 TRIA-LCAP-0321-0379 Active Endpoint License
20 TRIA-LCAP-0418-0040 Active Endpoint License
21 TRIA-LCAP-0776-0000 Active Endpoint License
22 TRIA-LCAP-0585-0801 Active Endpoint License
23 TRIA-LCAP-0959-0150 Active Endpoint License
24 TRIA-LCAP-0122-0469 Active Endpoint License
25 TRIA-LCAP-0940-0520 Active Endpoint License
26 TRIA-LCAP-0582-0703 Active Endpoint License
27 TRIA-LCAP-0494-0324 Active Endpoint License
28 TRIA-LCAP-0534-0242 Active Endpoint License
29 TRIA-LCAP-0897-0786 Active Endpoint License
30 TRIA-LCAP-0237-0194 Active Endpoint License
31 TRIA-LCAP-0623-0769 Active Endpoint License
32 TRIA-LCAP-0863-0076 Active Endpoint License
33 TRIA-LCAP-0459-0326 Active Endpoint License
34 TRIA-LCAP-0609-0780 Active Endpoint License
35 TRIA-LCAP-0706-0027 Active Endpoint License
Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.
Ready Version 4.4.0.4

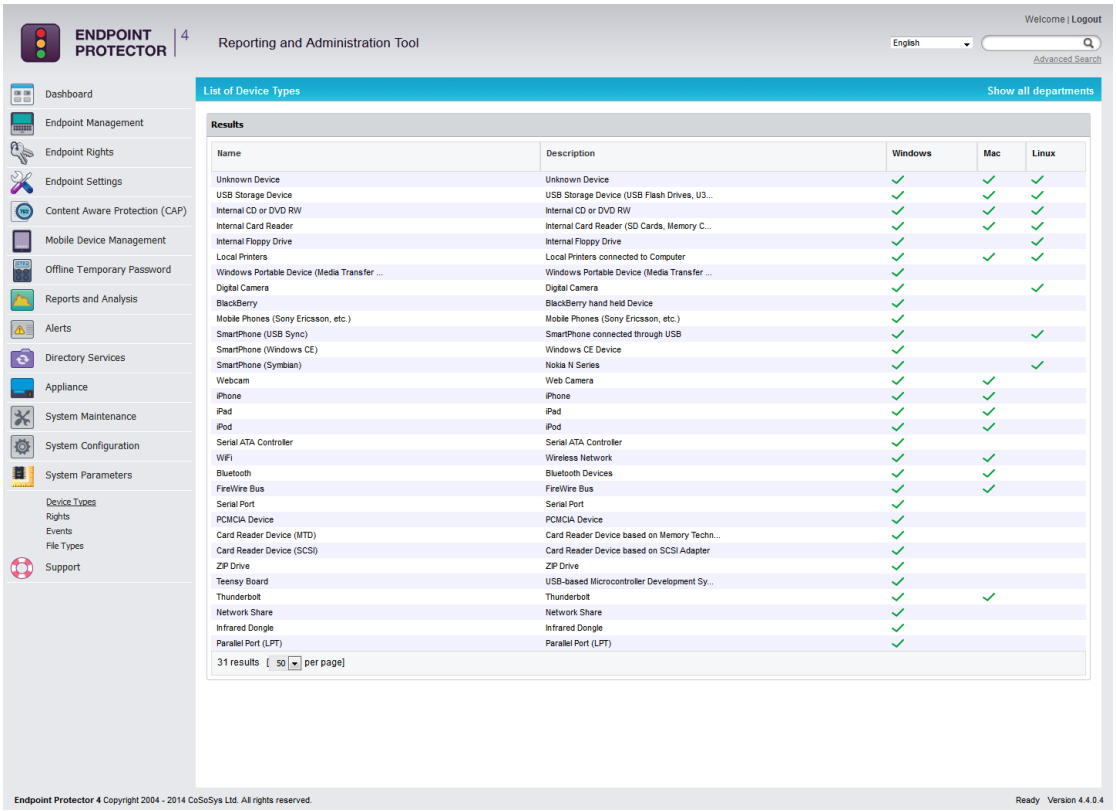
13. System Parameters

This module of Endpoint Protector is designed for super administrators. The advanced settings available here determine the functionality of the entire system.

Many of these parameters should be left untouched, on the default installation settings. Introducing wrong values can limit the functionality and performance of the entire system.

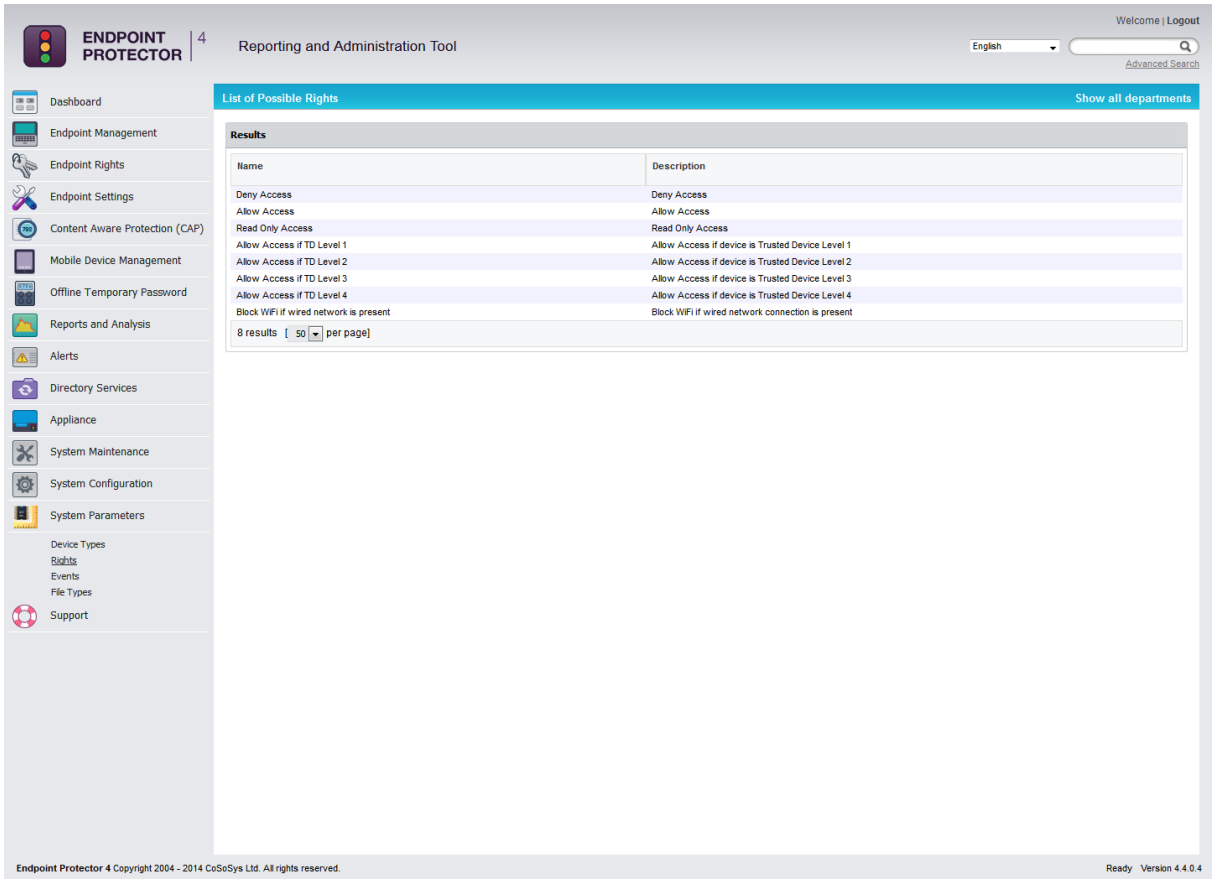
13.1. Device Types

Here is a list of all device types currently supported by Endpoint Protector, along with a short description for all of the items.



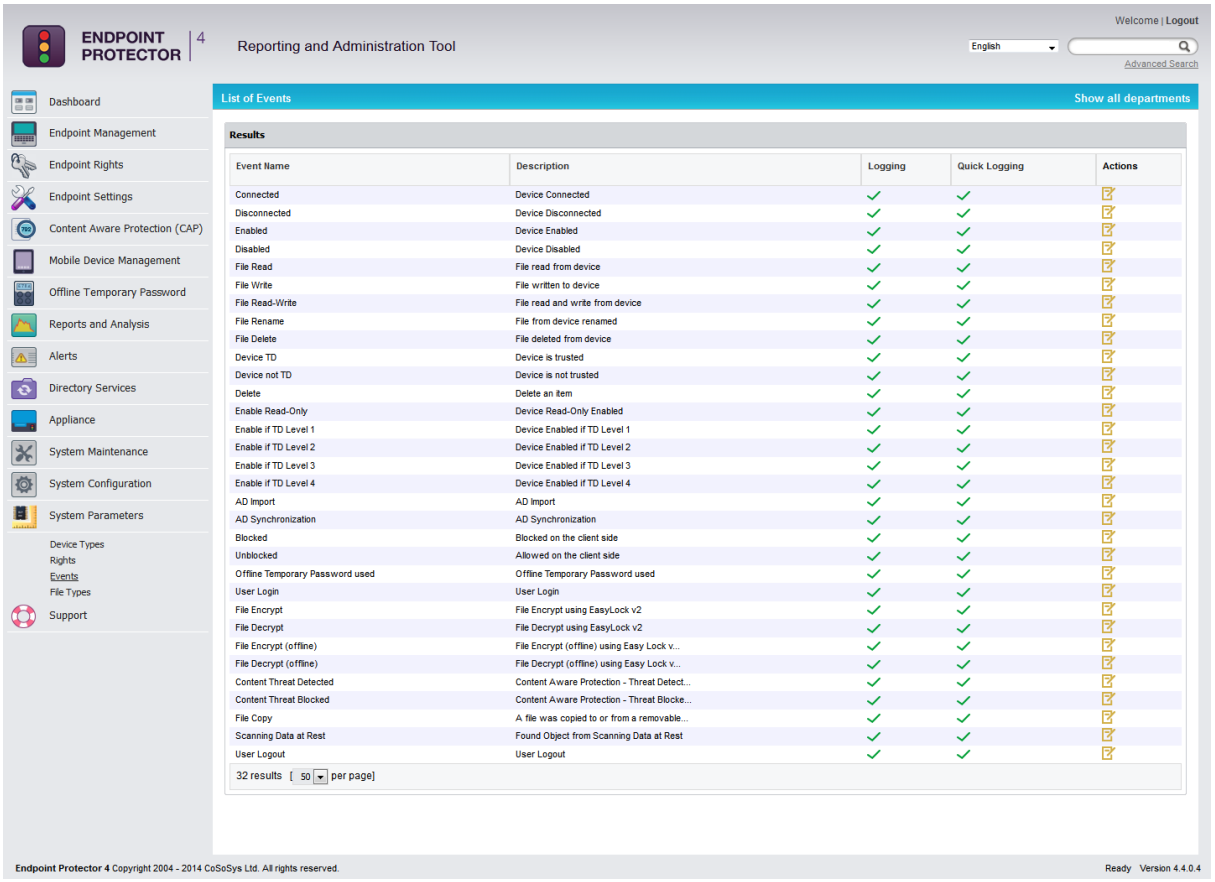
13.2. Rights

This list contains the rights which can be assigned on the system at any time.



13.3. Events

This list contains the events which will be logged for further reference.

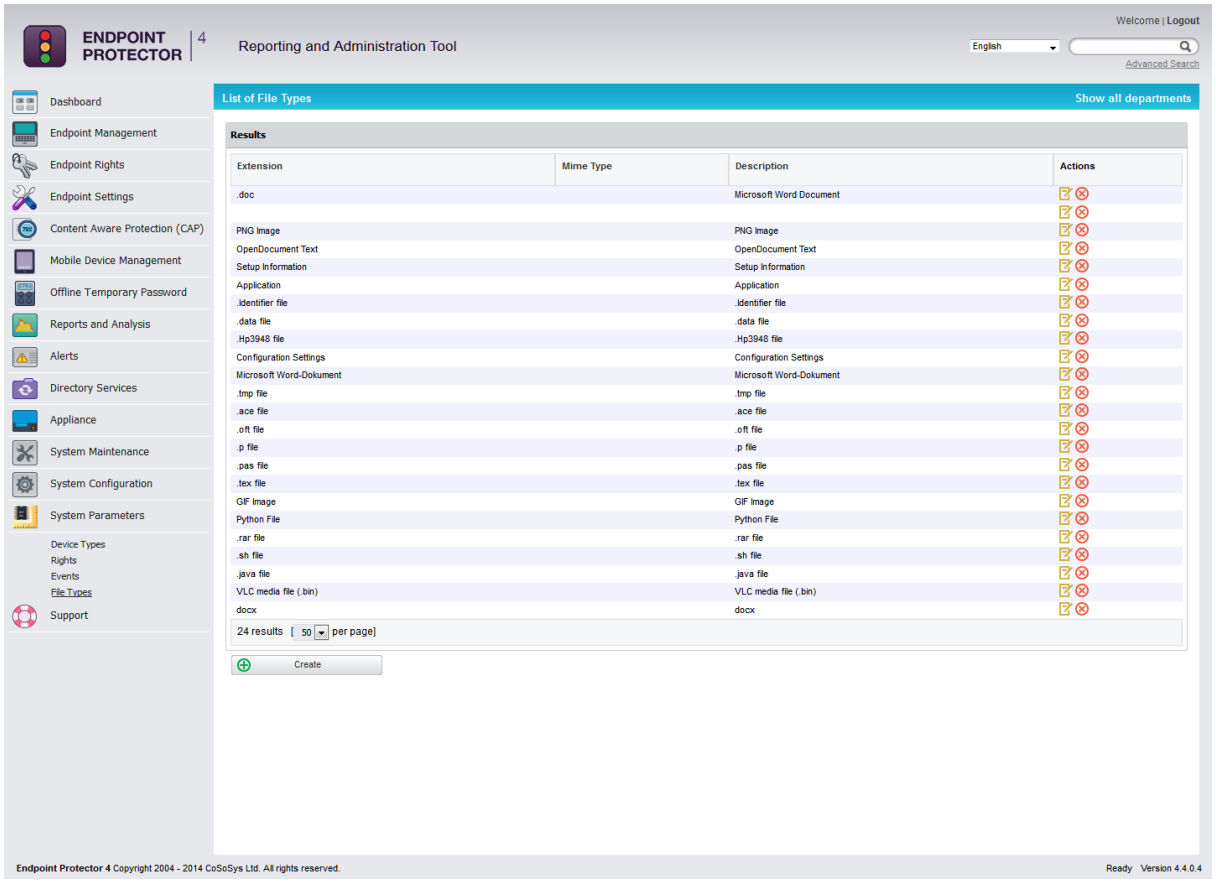


Note!

Changing this list without CoSoSys' acknowledgement can limit system functionality and performance; however, such customizations/implementations can be performed by request by one of our specialists as part of our Professional Services offered to customers.

13.4. File Types

This list contains common file type extensions and a description for each of them making them easier to recognize when creating audits.



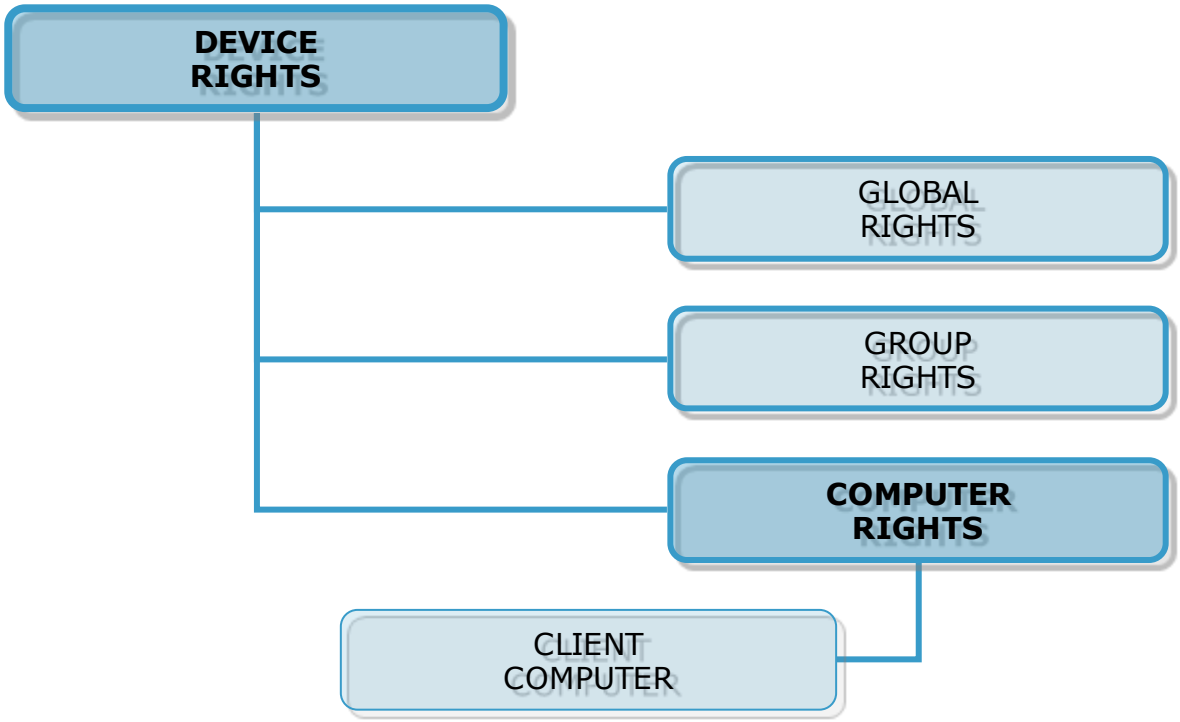
14. Setting up Policies

Most companies like to limit their employee's access to data, especially if it is confidential. Through Endpoint Protector you can enforce your security policies and keep confidential data away from the hands of curious employees. You can start setting your policies in the Rights section of Endpoint Protector. There are four sections here that need to be mentioned.

Device Rights, Computer Rights, Group Rights and Global Rights. You can find descriptions of these items in the previous paragraphs. Before configuring computers and devices, there are certain aspects of Endpoint Protector you should be aware of.

Computer Rights, Group Rights and Global Rights form a single unit and they inherit each-others settings, meaning that changes to any one of these modules affect the other ones. There are three levels of hierarchy: Global Rights, Group Rights and Computer Rights, the latter being the deciding factor in rights management.

The Device Rights module surpasses all settings from Computer Rights, Group Rights and Global Rights. If you give permission to a device to be available to clients, it will be usable under any circumstances.

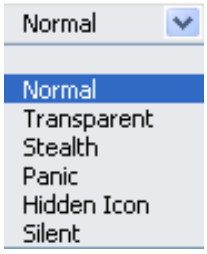


For example: in Global Rights, assign Allow for device X. If in Computer Rights, the same device does not have permission to be used; the device will not be usable. Same applies vice-versa: if the device lacks permission to be used in Global Rights, and has permission under Computer Rights, the device will be usable to the client. The same applies for Global Rights and Group Rights: if under Global Rights the device does not have permission to be used, and under Group Rights permission exists, the device will be available to the client.

	DEVICE 1	DEVICE 2	DEVICE 3	DEVICE 4	DEVICE 5	DEVICE 6
GLOBAL RIGHTS	NOT ALLOWED	ALLOWED	NOT ALLOWED	ALLOWED	NOT ALLOWED	ALLOWED
GROUP RIGHTS	NOT ALLOWED	NOT ALLOWED	ALLOWED	NOT ALLOWED	ALLOWED	ALLOWED
COMPUTER RIGHTS	ALLOWED	NOT ALLOWED	NOT ALLOWED	ALLOWED	ALLOWED	NOT ALLOWED
CLIENT COMPUTER	ALLOWED	NOT ALLOWED	NOT ALLOWED	ALLOWED	ALLOWED	NOT ALLOWED

15. Modes for Users, Computers and Groups

Endpoint Protector features several functionality modes for users, computers and groups. These modes are accessible for each item (users, computers, groups) from the System Policies module of Endpoint Protector using the "Edit" button.



You can change these at any given time.

There are six modes from which you can choose:

- Normal Mode (default setting of Endpoint Protector)
- Transparent Mode
- Stealth Mode
- Panic Mode
- Hidden Icon Mode
- Silent Mode

15.1. Transparent Mode

This mode is used if you want to block all devices but you don’t want the user to see and know anything about EPP activity.

- no system tray icon is displayed
- no system tray notifications are shown
- everything is blocked regardless if authorized or not
- Administrator receives alerts (dashboard also shows alerts) for all activities

15.2. Stealth Mode

Similar to Transparent mode, Stealth mode allows the administrator to monitor all of the users and computers activities and actions with all devices allowed.

- no system tray icon is displayed
- no system tray notifications are shown
- everything is allowed (nothing is blocked regardless of what activity)
- file shadowing and file tracing are enabled to see and monitor all user activity
- Administrator receives alerts (dashboard shows also alerts) for all activities

15.3. Panic Mode

Under special circumstances, Panic Mode can be set manually by the administrator in order to block all access to devices.

- system tray icon is displayed
- notifications are displayed
- everything is blocked regardless if authorized or not
- Administrator receives alert (dashboard also shows alerts) when PCs are going in and out of Panic mode

15.4. Hidden Icon Mode

The Hidden Icon Mode is similar to the Normal mode, the difference consisting in the fact that the Agent is not visible to the user.

- no system tray icon is displayed
- no system tray notifications are shown
- all set rights and settings are applied

15.5. Silent Mode

The Silent Mode is similar to the Normal mode, the difference consisting in the fact that the notifications do not pup-up to the user.

- system tray icon is displayed
- no system tray notifications are shown
- all set rights and settings are applied

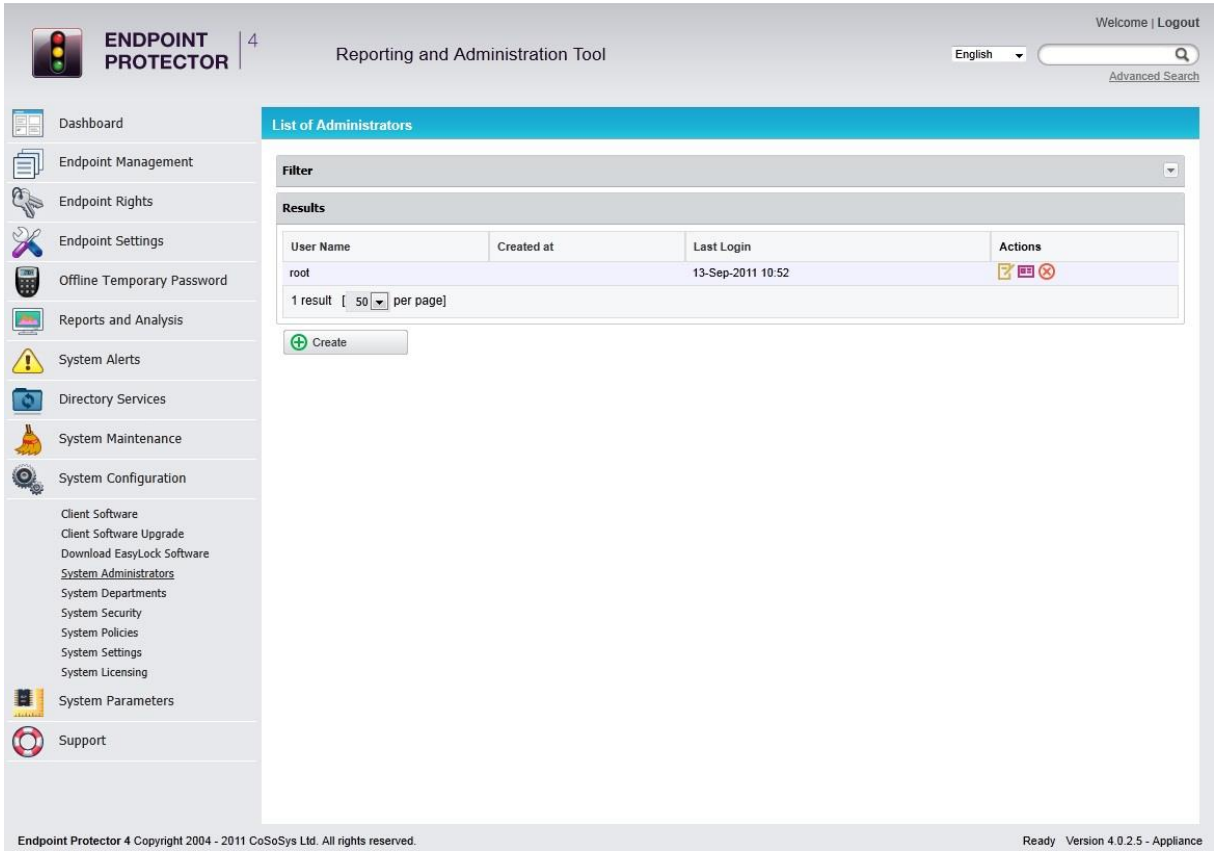
15.6. Adding new administrator(s)

You can add an unlimited number of system administrators, depending on the size and manageability of your network.

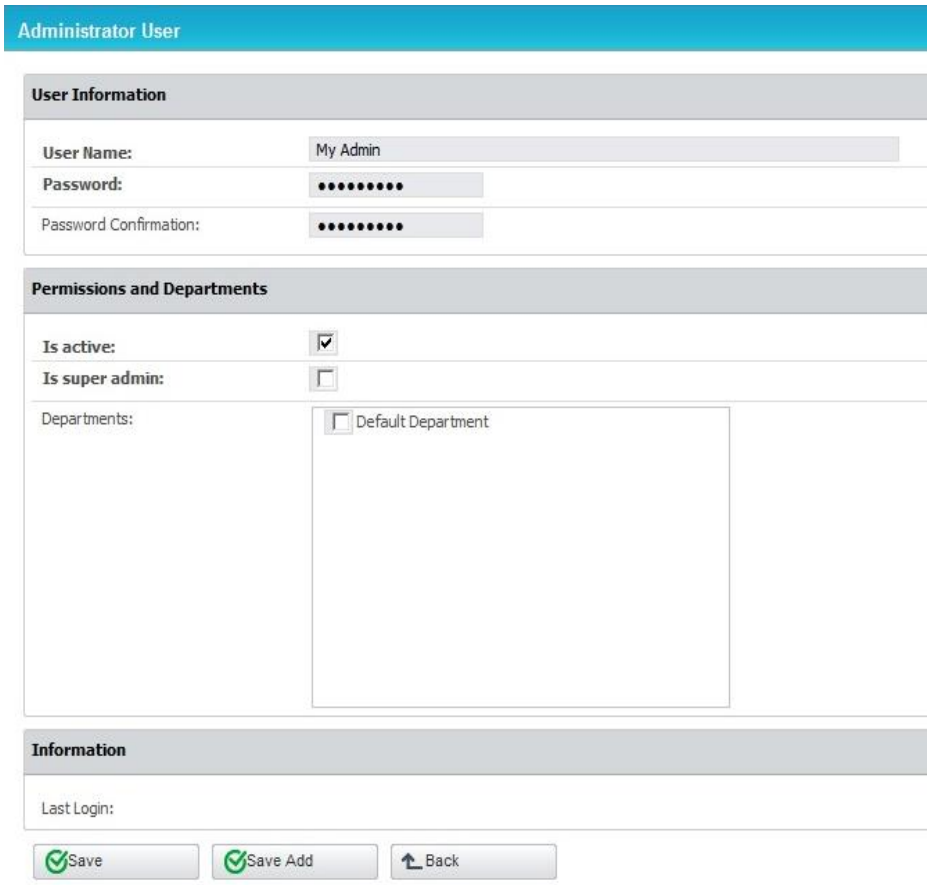
While fewer administrators are recommended for easier data loss prevention, it is easier to manage a large network with more.

To add an administrator or Super Administrator in Endpoint Protector, you must login as a super administrator and access the "System Configuration" module then the "Administrators" panel.

Here you can see a list of current Administrator and Super Administrators.



To add another Administrator or Super Administrator, click the "Create" button.



Enter the desired user name and password for the new account, then set if the account is active or not or whether is a super admin or not.

Is active – if this option is not enabled the selected user cannot log in to the Endpoint Protector console. Use this option in case you want to create temporary admin or super admin privileges to a certain user and then remove them or if you want to disable an administrator but do not want to delete his credentials from the server.

Is Super Admin – Super Administrators have more rights than administrators. Super Administrator can create, delete and modify administrator and super administrator settings, while standard administrators do not have this right. The most important difference is that only super administrators are able to view the "Reports and Analysis" section if the option "Data Security Privileges" is selected.

15.7. Working with logs and reports

Endpoint Protector creates a device activity log in which it records actions from all clients and devices connected along with all administrative actions such as device authorizations, giving a history for devices, PCs and users for future audits and detailed analysis.

Logs Report - The most powerful and detailed representation of activity recording can be achieved using this module. This allows the administrator to see exactly which device, computer a user used on a specific time interval, and whether the shadowing for that user/device is enabled or not. There is a special filter designed to make it easier to find this information.

Online Users – Online users are end users who have logged on to a client computer.

Online Computers – Online Computers are client computers which have been set up to communicate with the Endpoint Protector server by installing the Endpoint Protector Client. Here you can see a list of computers which are currently powered on and you can view the actions they have taken.

Online Devices – Connected Devices are devices which are currently plugged-in to one of the (online) client computers. Here again you have the possibility to view an activity log, this time, of the device.

Statistics – The statistics module can generate reports on registered computers, devices and users based on traffic, connections or overall activity. You can set a period for this report (last week, month or year).

16. Enforced Encryption with Trusted Devices

Protecting Data in Transit is essential to ensure no third party has access to data in case a device is lost or stolen. The Enforced Encryption solution gives administrators the possibility to protect confidential data on portable devices in case of loss or theft. If a Trusted Device fails to get authorization from the Endpoint Protector 4 Server, it will not be usable.

How does it work?

Enforcing Encryption can be done by utilizing Trusted Devices. Trusted Devices must receive authorization from the Endpoint Protector 4 Server, otherwise they will be unusable.

There are four levels of security for Trusted Devices:

- **Level 1** - Minimum security for office and personal use with a focus on software based encryption for data security. Offers companies already regulatory compliance.
  Any USB Flash Drive and most other portable storage devices can be turned into a Trusted Device Level 1 with EasyLock Software from CoSoSys.
  No hardware upgrade is required.
  http://www.endpointprotector.com/en/index.php/products/easylock

- **Level 2** - Medium security level with biometric data protection or advanced software based data encryption.
  Requires special hardware that includes security software and that has been tested for Trusted Device Level 2.
  Hardware is widely available in retail stores.

- **Level 3** - High security level with strong hardware based encryption that is mandatory for sensitive enterprise data protection for regulatory

compliance such as SOX, HIPAA, GBLA, PIPED, Basel II, DPA, or PCI 95/46/EC.
Requires special hardware that includes advanced security software and hardware based encryption and that has been tested for Trusted Device Level 3.

- **Level 4** - Maximum security for military, government and even secret agent use. Level 4 Trusted Devices include strong hardware based encryption for data protection and are independently certified (e.g. FIPS 140). These devices have successfully undergone rigorous testing for software and hardware.
  Requires special hardware that is available primarily through security focused resellers.

16.1. How a Level 1 Trusted Device Works

User connects Device to Endpoint Protector protected Client PC. Device is blocked by Endpoint Protector (default action).

Device is checked for authorization.

If device is an authorized Trusted Device Level 1, the EasyLock software on Device will automatically open.

User can transfer files via Drag & Drop in EasyLock from the PC to the Trusted Device.

Data transferred to devices is encrypted via 256bit AES.

User cannot access the device using Windows Explorer or similar applications (e.g. Total Commander).

User does not have the possibility to copy data in unencrypted state to the Trusted Device.

“Trusted Device” implies that the devices offer a safe, risk-free environment to transfer sensitive data and tracking or shadowing files and file transfers is not needed for these devices.

Administrator can audit what user, with what device, on what PC, has transferred what files.

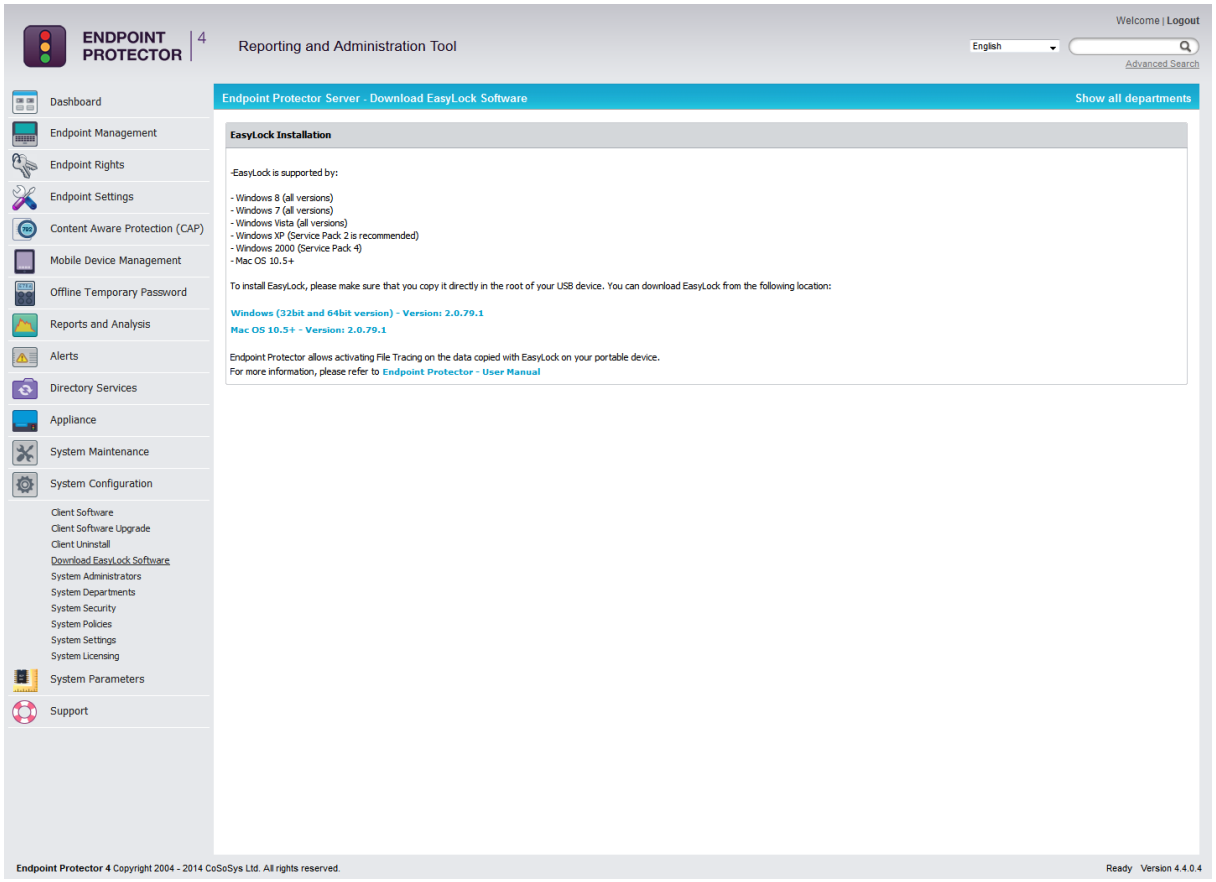
Note!

EasyLock will auto-play only on Windows OS.

16.2. EasyLock Software for Trusted Devices Level 1

EasyLock allows portable devices to be identified as Trusted Devices and protects data on the device with government-approved 256bit AES CBC-mode encryption. With the intuitive Drag & Drop interface, files can be quickly copied to and from the device.

EasyLock can be downloaded directly from the EasyLock Software panel under the System Configuration module.


ENDPOINT PROTECTOR 4
Reporting and Administration Tool
Welcome | Logout
English
Advanced Search
Dashboard
Endpoint Management
Endpoint Rights
Endpoint Settings
Content Aware Protection (CAP)
Mobile Device Management
Offline Temporary Password
Reports and Analysis
Alerts
Directory Services
Appliance
System Maintenance
System Configuration
Client Software
Client Software Upgrade
Client Uninstall
Download EasyLock Software
System Administrators
System Departments
System Security
System Policies
System Settings
System Licensing
System Parameters
Support
Endpoint Protector Server - Download EasyLock Software
Show all departments
EasyLock Installation
-EasyLock is supported by:
- Windows 8 (all versions)
- Windows 7 (all versions)
- Windows Vista (all versions)
- Windows XP (Service Pack 2 is recommended)
- Windows 2000 (Service Pack 4)
- Mac OS 10.5+
To install EasyLock, please make sure that you copy it directly in the root of your USB device. You can download EasyLock from the following location:
Windows (32bit and 64bit version) - Version: 2.0.79.1
Mac OS 10.5+ - Version: 2.0.79.1
Endpoint Protector allows activating File Tracing on the data copied with EasyLock on your portable device.
For more information, please refer to Endpoint Protector - User Manual
Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.
Ready Version 4.4.0.4

To install EasyLock on an USB Flash drive one has to copy the file to the root folder of a partition associated with that device. For Windows computers the file is "EasyLock.exe" and for Macs the file is “EasyLock.app”

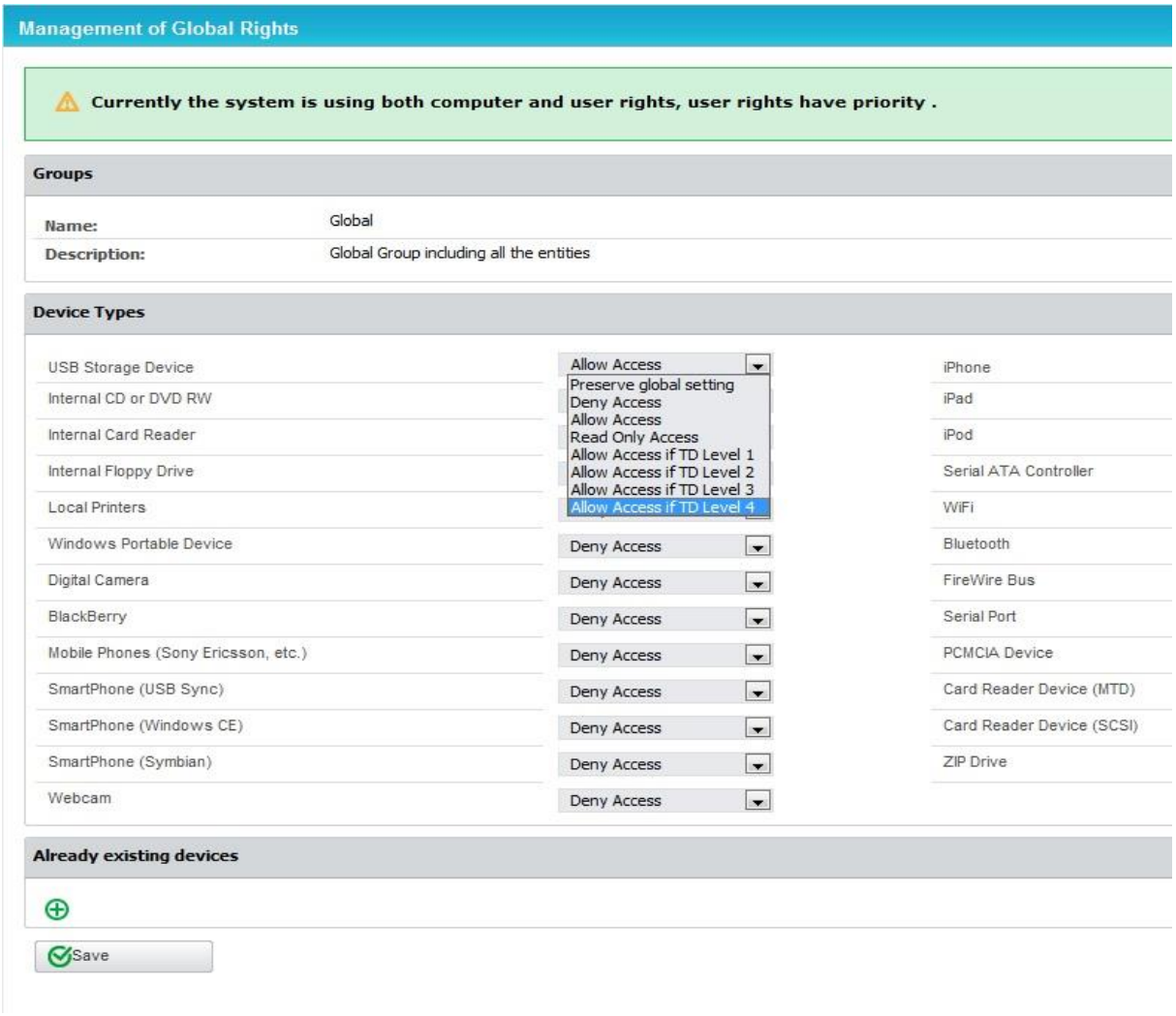
16.2.1. Managing Trusted Devices from EPP server console

Access to Trusted Devices can be configured from the Global Rights module of Endpoint Protector 4, under Rights tab.

Access the drop-down box next to USB Storage Device and select the desired level of Trusted Devices you wish to grant access to.

More information about EasyLock:

http://www.endpointprotector.com/en/index.php/products/easylock



16.2.2. File Tracing on EasyLock 2 TrustedDevices

Endpoint Protector 4 allows tracing of files copied in an encrypted way with EasyLock 2 on portable devices. This option can be activated from inside the System Settings window located under the System Configuration tab.

By checking the File Tracing option, all data transferred to and from devices using EasyLock 2 is recorded and logged for later auditing. The logged information is automatically sent to Endpoint Protector Server if Endpoint Protector Client is present on that computer, this taking place regardless of the File Tracing option being enabled or not for that specific computer.

In case that Endpoint Protector Client is not present, the information is stored locally in an encrypted format on the device and it will be sent at a later time from any other computer with Endpoint Protector Client installed.

The additional "Offline File Tracing" option is an extension to the first option, offering the possibility to store information directly on the device, before being sent to the Endpoint Protector Server. The list of copied files is sent only next time the device is plugged in and only if Endpoint Protector Client is present and communicates with Endpoint Protector Server, this allowing the transfer and offering a performance based improvement to the overall system functionality.

Additionally, Easy Lock 2 performs File Shadowing for the files that are transferred, if Endpoint Protector Client is present and the File Shadowing option is enabled on the computer on which the events occur. This is a real time event and no shadowing information is stored on the device at any given time.

Note!

File Tracing on EasyLock 2 Trusted Devices must be enabled separately from inside the System Settings window. Enabling global File Tracing will not automatically activate the File Tracing option on EasyLock 2 Trusted Devices and vice versa. Bare in mind that The File Tracing feature on EasyLock 2 Trusted Devices is available at the moment only for Windows OS.

17. Endpoint Protector Client

The Endpoint Protector Client is the application which once installed on the client Computers (PC's), communicates with the Endpoint Protector Server and blocks or allows devices to function, as well as sends out notifications in case of unauthorized access.

17.1. Endpoint Protector Client Installation

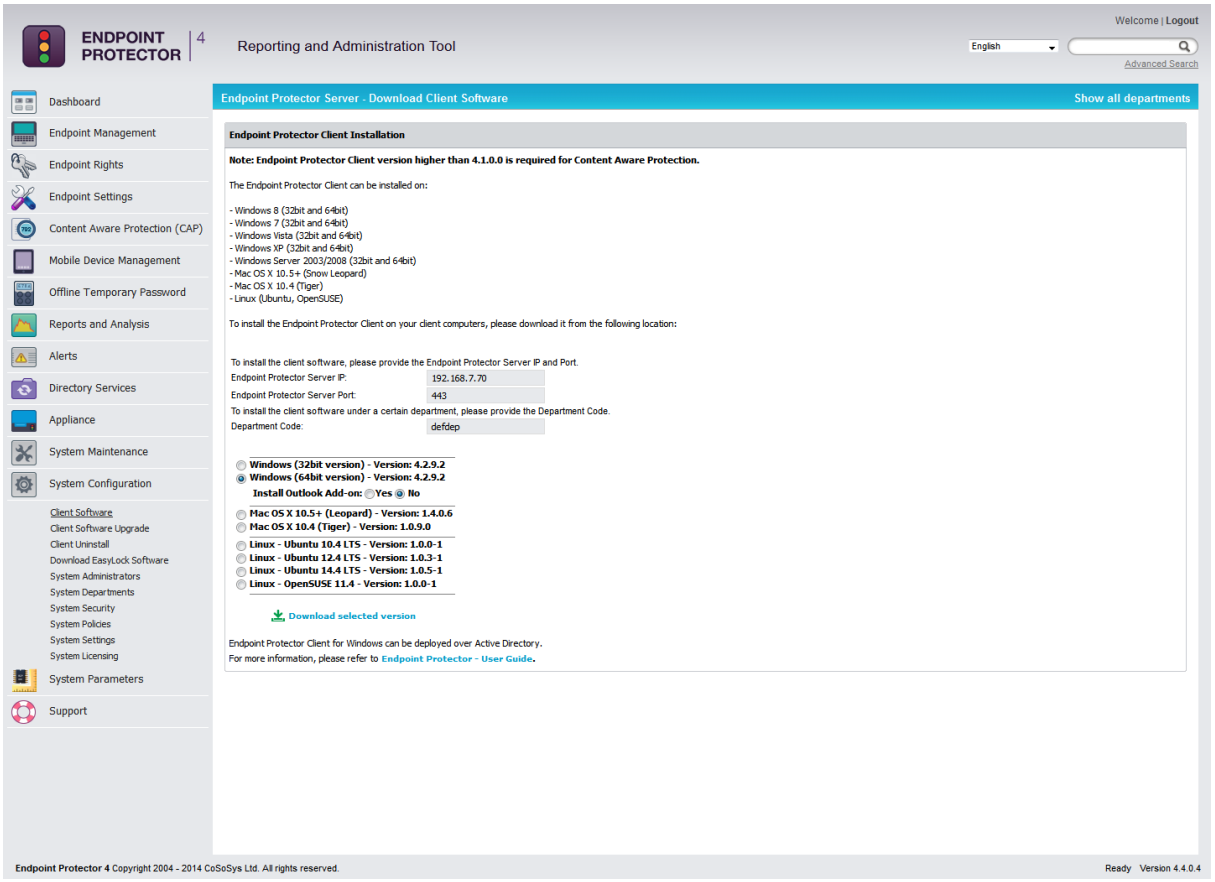
To install the Endpoint Protector Client on your client computers, you can download it directly from the Endpoint Protector Server Web interface, under the System Configuration -> Client Software tab.

Note!

You need to "Save" the Endpoint Protector Client first on a location and then install it from there. Do not run it directly from the browser!

File Download - Security Warning
Do you want to run or save this file?
Name: EPPClientSetup_x86_32.msi
Type: Windows Installer Package, 4.24MB
From:
Run
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Before downloading the Endpoint Protector Client, please make sure that you specify the IP of your Endpoint Protector Server and the unique code of the Department in which you want to include it. In case that no unique code is entered, the client will be assigned to the Default Department.


ENDPOINT PROTECTOR 4
Reporting and Administration Tool
Welcome | Logout
English
Advanced Search
Dashboard
Endpoint Management
Endpoint Rights
Endpoint Settings
Content Aware Protection (CAP)
Mobile Device Management
Offline Temporary Password
Reports and Analysis
Alerts
Directory Services
Appliance
System Maintenance
System Configuration
Client Software
Client Software Upgrade
Client Uninstall
Download EasyLock Software
System Administrators
System Departments
System Security
System Policies
System Settings
System Licensing
System Parameters
Support
Endpoint Protector Server - Download Client Software
Show all departments
Endpoint Protector Client Installation
Note: Endpoint Protector Client version higher than 4.1.0.0 is required for Content Aware Protection.
The Endpoint Protector Client can be installed on:
- Windows 8 (32bit and 64bit)
- Windows 7 (32bit and 64bit)
- Windows Vista (32bit and 64bit)
- Windows XP (32bit and 64bit)
- Windows Server 2003/2008 (32bit and 64bit)
- Mac OS X 10.5+ (Snow Leopard)
- Mac OS X 10.4 (Tiger)
- Linux (Ubuntu, OpenSUSE)
To install the Endpoint Protector Client on your client computers, please download it from the following location:
To install the client software, please provide the Endpoint Protector Server IP and Port.
Endpoint Protector Server IP: 192.168.7.70
Endpoint Protector Server Port: 443
To install the client software under a certain department, please provide the Department Code.
Department Code: defdep
Windows (32bit version) - Version: 4.2.9.2
Windows (64bit version) - Version: 4.2.9.2
Install Outlook Add-on: Yes No
Mac OS X 10.5+ (Leopard) - Version: 1.4.0.6
Mac OS X 10.4 (Tiger) - Version: 1.0.9.0
Linux - Ubuntu 10.4 LTS - Version: 1.0.0-1
Linux - Ubuntu 12.4 LTS - Version: 1.0.3-1
Linux - Ubuntu 14.4 LTS - Version: 1.0.5-1
Linux - OpenSUSE 11.4 - Version: 1.0.0-1
Download selected version
Endpoint Protector Client for Windows can be deployed over Active Directory.
For more information, please refer to Endpoint Protector - User Guide.
Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.
Ready Version 4.4.0.4

Active Directory can be used for Endpoint Protector Client deployment as well. This feature can be found in the Endpoint Protector System Configuration menu Active Directory.

Note!

For Linux clients, please consult the readme file available under the "Read this before installing" link for exact installation instructions corresponding to the previously selected Linux distribution!

17.2. Endpoint Protector Client Security

The Endpoint Protector Client has a built in security system which makes stopping the service nearly impossible.

This mechanism has been implemented to prevent the circumvention of security measures enforced by then network administrator.

17.3. Client Notifications (Notifier)

The Endpoint Protector Client, depending in the mode it is currently running on, will display a notification from the taskbar icon when an unauthorized device is connected to the PC. Not only does it log any attempts to forcefully access the system, it can also trigger the Panic mode.

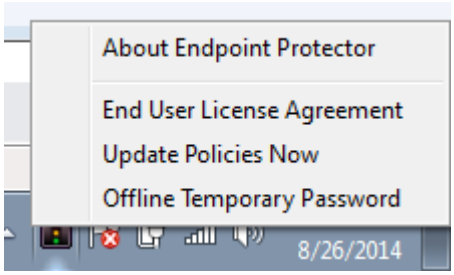
Security Warning - Endpoint Protector
An unauthorized device was connected to this PC.
Remove the device now or contact the PCs administrator for authorization.

In case of a Mac, the notification will look like bellow:

(78%)
Fri 9:39 AM
Security Warning
An unauthorized device was connected to this computer. Remove the device now or contact the computer's administrator for authorization.
Kingmax USB2.0 FlashDisk

17.4. Client Policy Update

The Client has a built in feature to ensure the latest policies are received. The "Update Policies Now" is available by right clicking on the Endpoint Protector system tray icon, as shown below:



17.5. Offline Functionality for Endpoint Protector Client

Depending on the global settings the Endpoint Protector Client will store a local file tracing history and a local file shadow history that will be submitted and synchronized with the Endpoint Protector Server upon next connection to the network.

17.6. DHCP / Manual IP address

Endpoint Protector Client automatically recognizes changes in the network's configuration and updates settings accordingly, meaning that you can keep your laptop protected at the office (DHCP) and at home(Manual IP address) too without having to reinstall the client or modify any changes.

17.7. Client Removal

17.7.1. Client Removal on Windows OS

The Endpoint Protector Client cannot be uninstalled without specifying the password set by the administrator(s) in the Reporting and Administration Tool.

There is also the option to remotely uninstall clients from the

17.7.2. Client removal on MAC OS X

To remove the Endpoint Protector Client you need to run (double click in Finder) the "remove-epp.command" file that was attached to the "Endpoint Protector" client package that you downloaded.

You will be prompted to enter the root password to perform administrative tasks.

17.7.3. Client removal on Linux OS

To remove the Endpoint Protector Client you need to run from the console/terminal the "uninstall.sh" file that was attached to the "Endpoint Protector" client package that you downloaded.

Note!

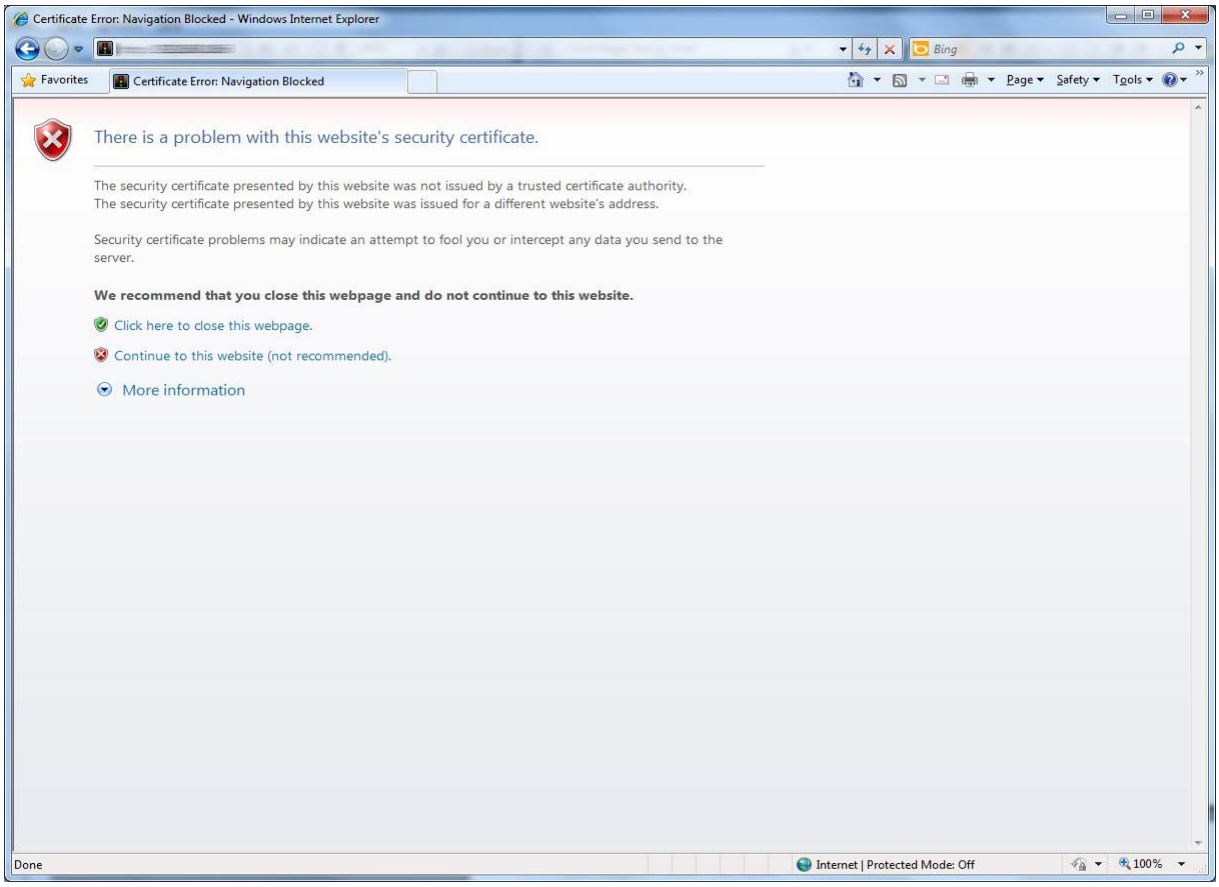
For exact uninstall instructions corresponding to your Linux distribution, please consult the readme file available in the System Configuration – Client Installation window by clicking the "Read this before installing" link!

18. Installing Root Certificates to your Internet Browser

18.1. For Microsoft Internet Explorer

Open Endpoint Protector Administration and Reporting Tool IP address. (Your Appliance static IP Address, example https://192.168.0.201).

If there is no certificate in your browser, you will be prompted with Certificate Error page like the screenshot below.


Certificate Error: Navigation Blocked - Windows Internet Explorer
Favorites
Certificate Error: Navigation Blocked
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information
Done
Internet | Protected Mode: Off
100%

Continue your navigation by clicking "Continue to this website (not recommended)".

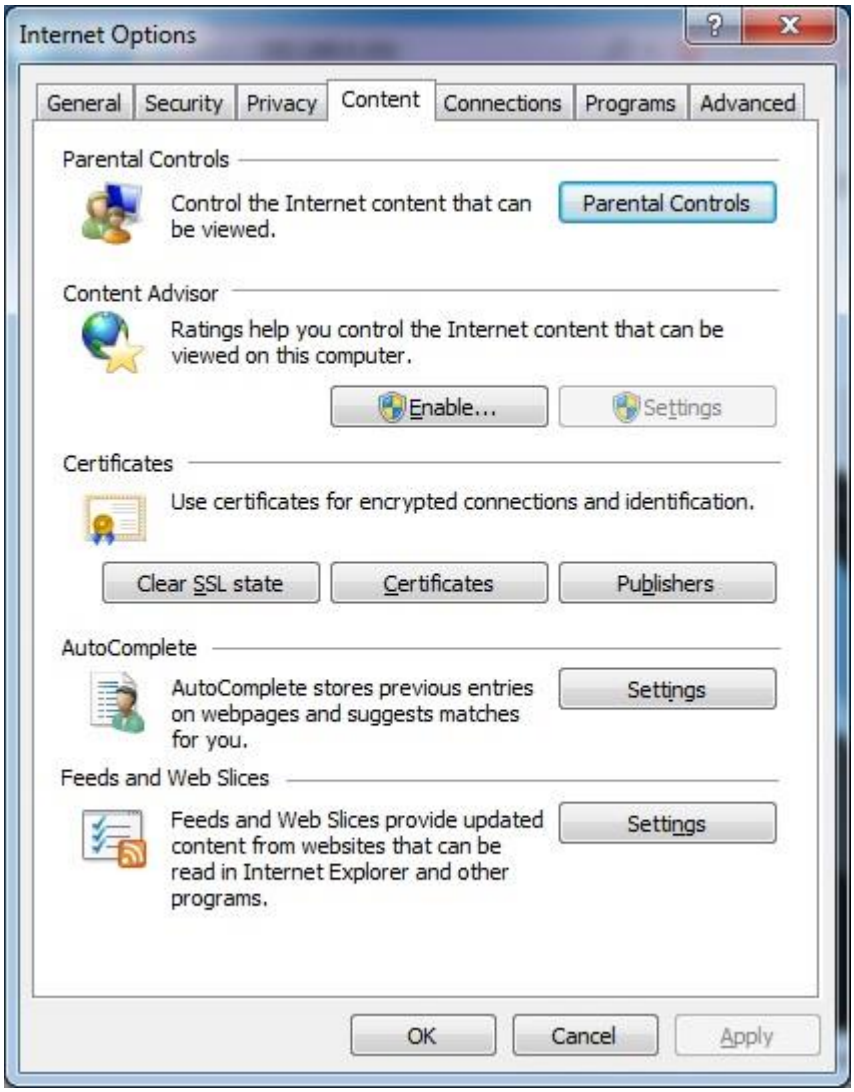
Now, go to the Certificate file you downloaded from the Appliance Setup Wizard->Appliance Server Certificate-> and install the Certificate.

Click the Certificate Error button just next to the IE address bar as shown.

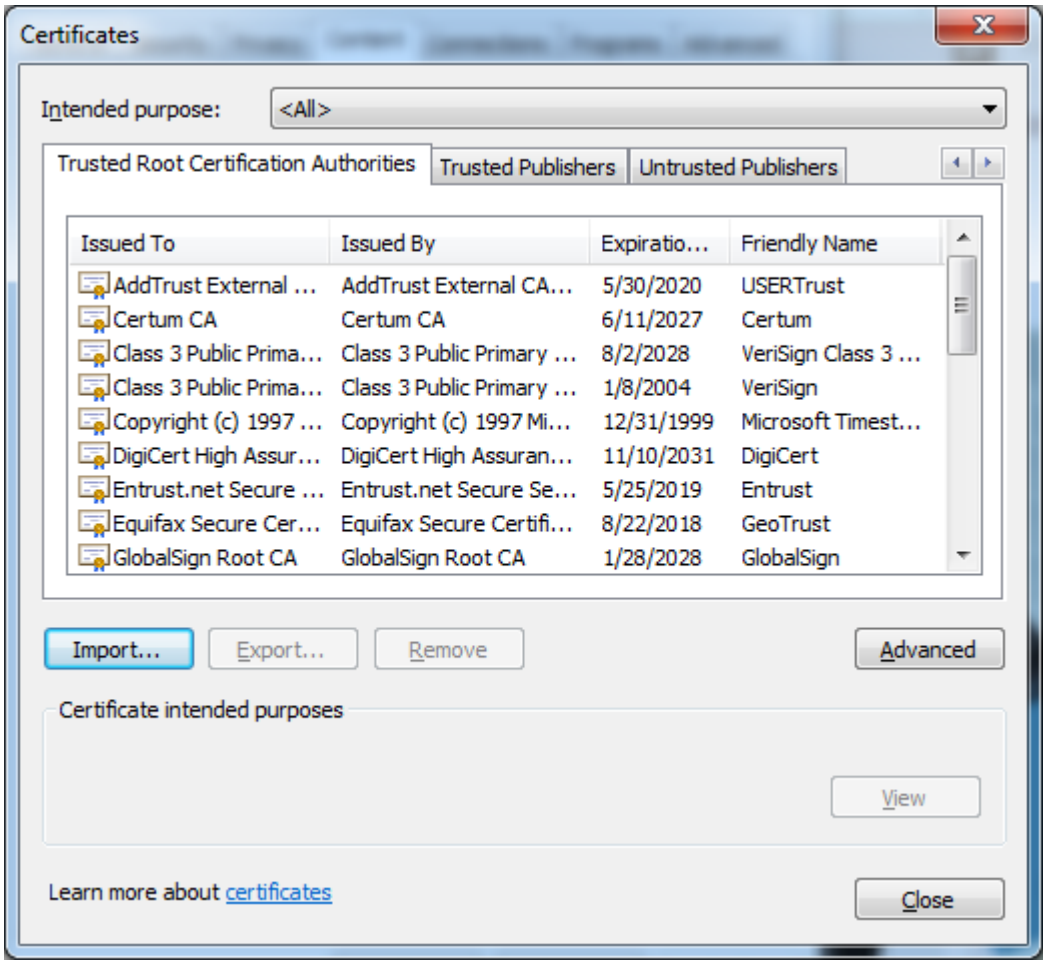
By clicking the "Certificate Error" button, a pop-up window appears. Just click the "View certificates" in that pop-up window.

Another pop-up Certificate window will appear with three tabs namely "General", "Details" and "Certification Path".

Select the "General" tab and then click "Install Certificate..." button or go to Tools->Internet Options-> Content->Certificates.



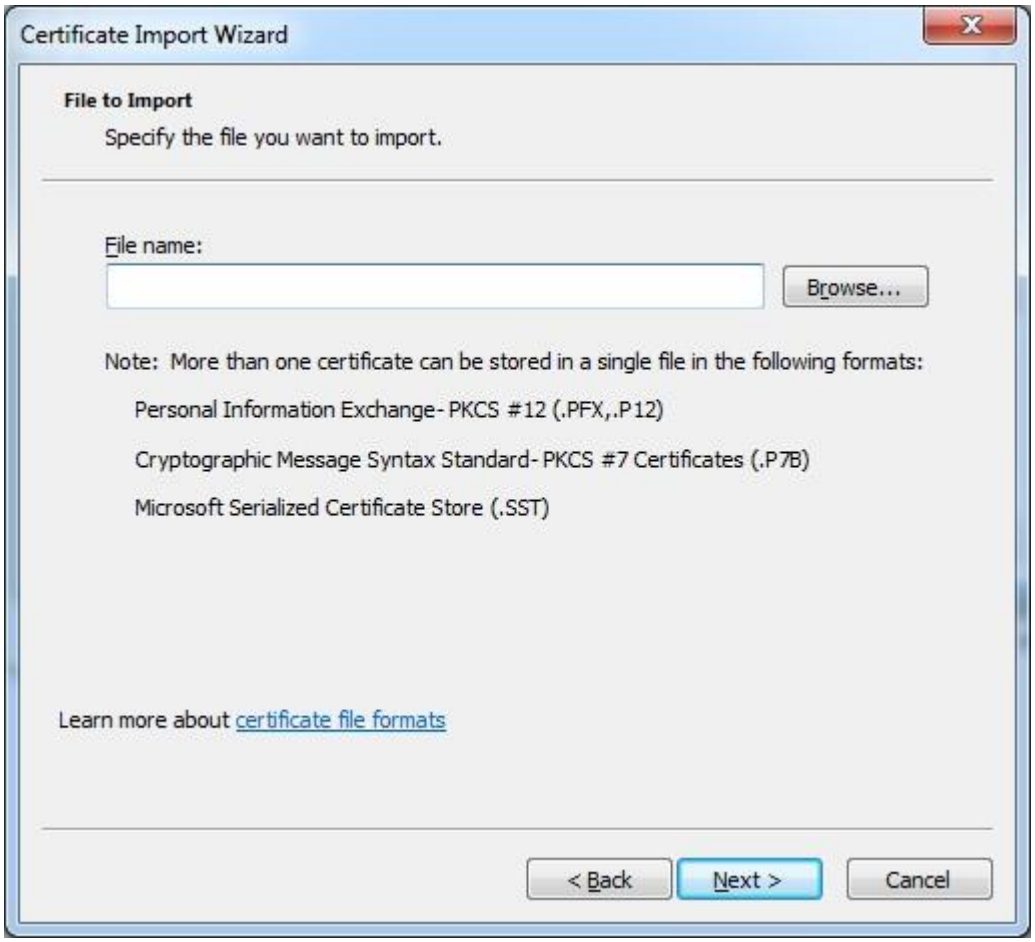
From the Certificates list, select "Trusted Root Certification Authorities" and click on the "Import" button.



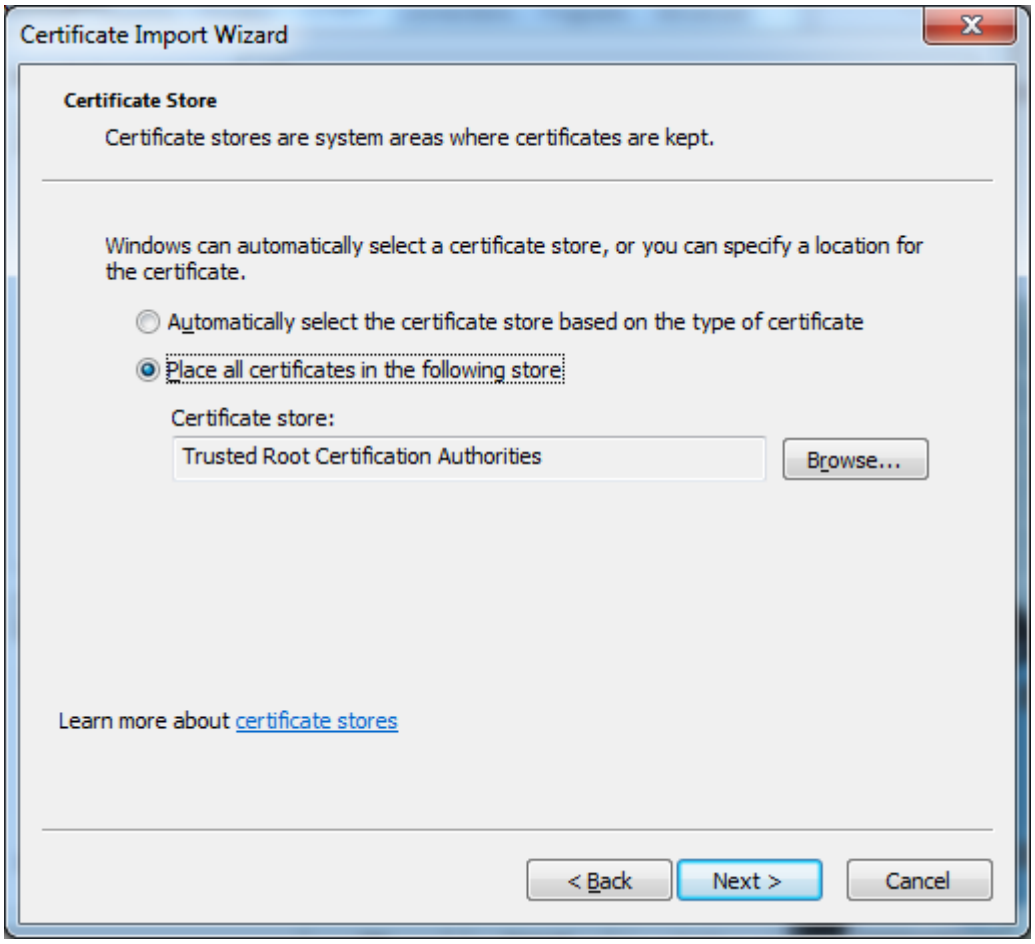
A Welcome to the Certificate Import Wizard pops up. Just click the Next button.

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

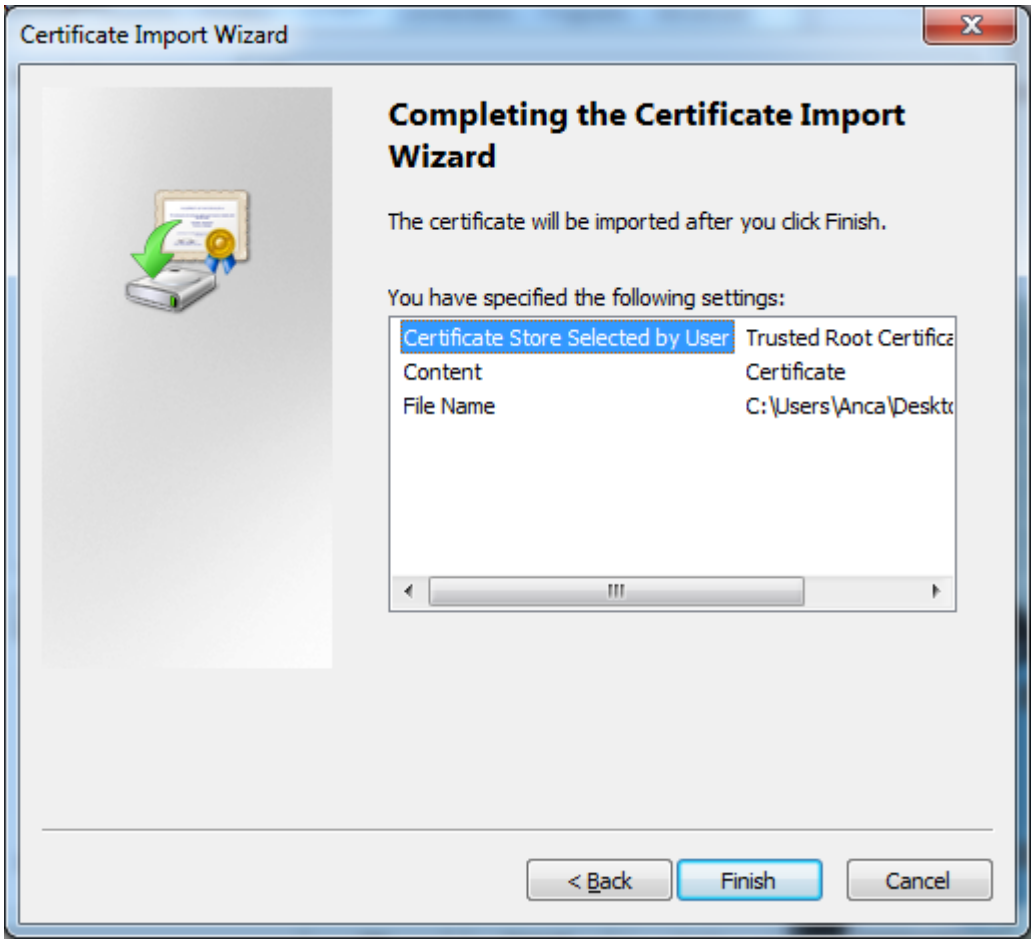
Browse for the Certificate file you downloaded from the Appliance Setup Wizard ->Appliance Server Certificate.


Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
Browse...
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
Learn more about certificate file formats
< Back
Next >
Cancel

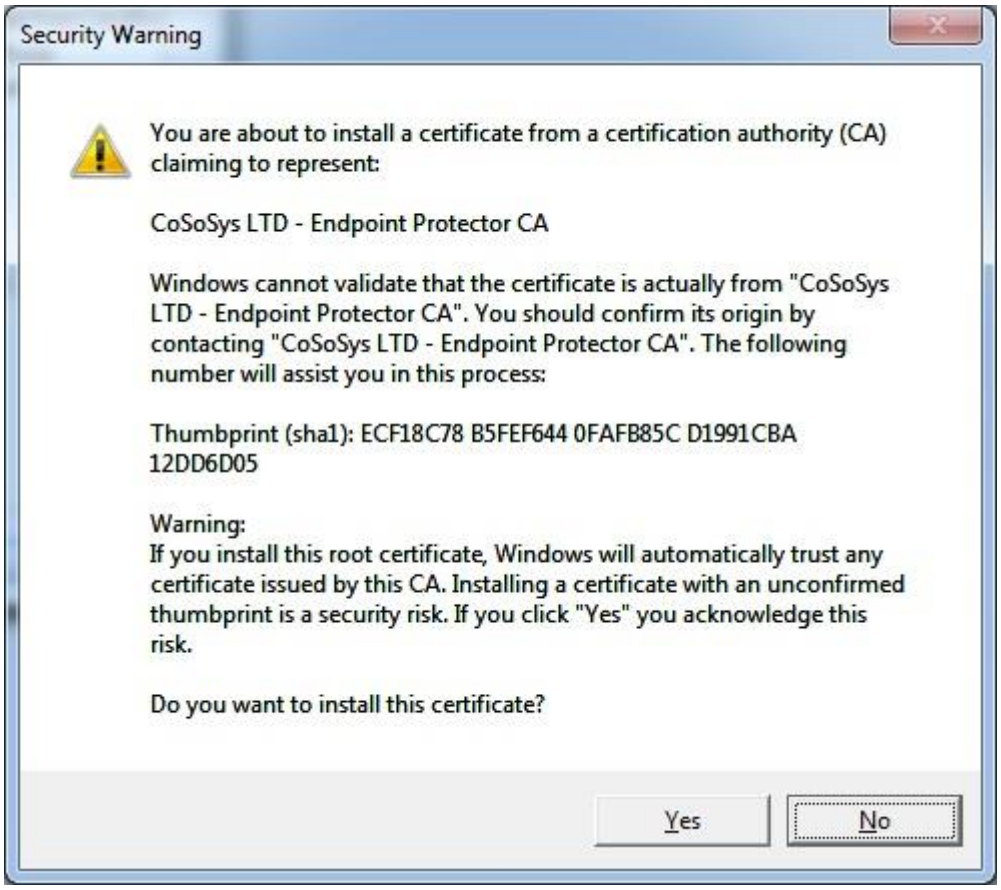
In the Certificate Store window, select "Place all certificates in the following store" radio button.


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Trusted Root Certification Authorities
Browse...
Learn more about certificate stores
< Back
Next >
Cancel

Another "Completing the Certificate Import Wizard" pops up. Just click the "Finish" button.

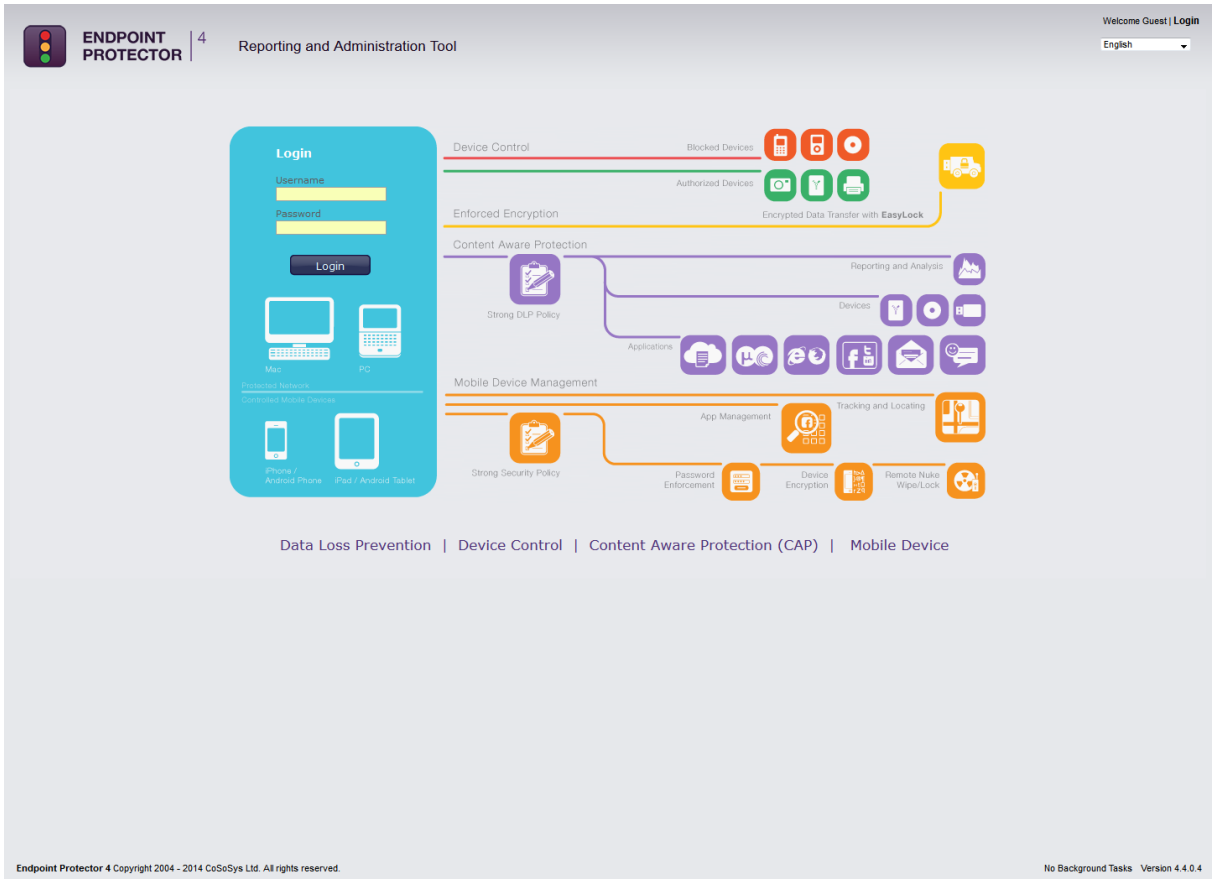


A Security Warning window pops up. Just click “Yes”.


Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
CoSoSys LTD - Endpoint Protector CA
Windows cannot validate that the certificate is actually from "CoSoSys LTD - Endpoint Protector CA". You should confirm its origin by contacting "CoSoSys LTD - Endpoint Protector CA". The following number will assist you in this process:
Thumbprint (sha1): ECF18C78 B5FEF644 0FAFB85C D1991CBA 12DD6D05
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No

You have now successfully installed the Certificate.

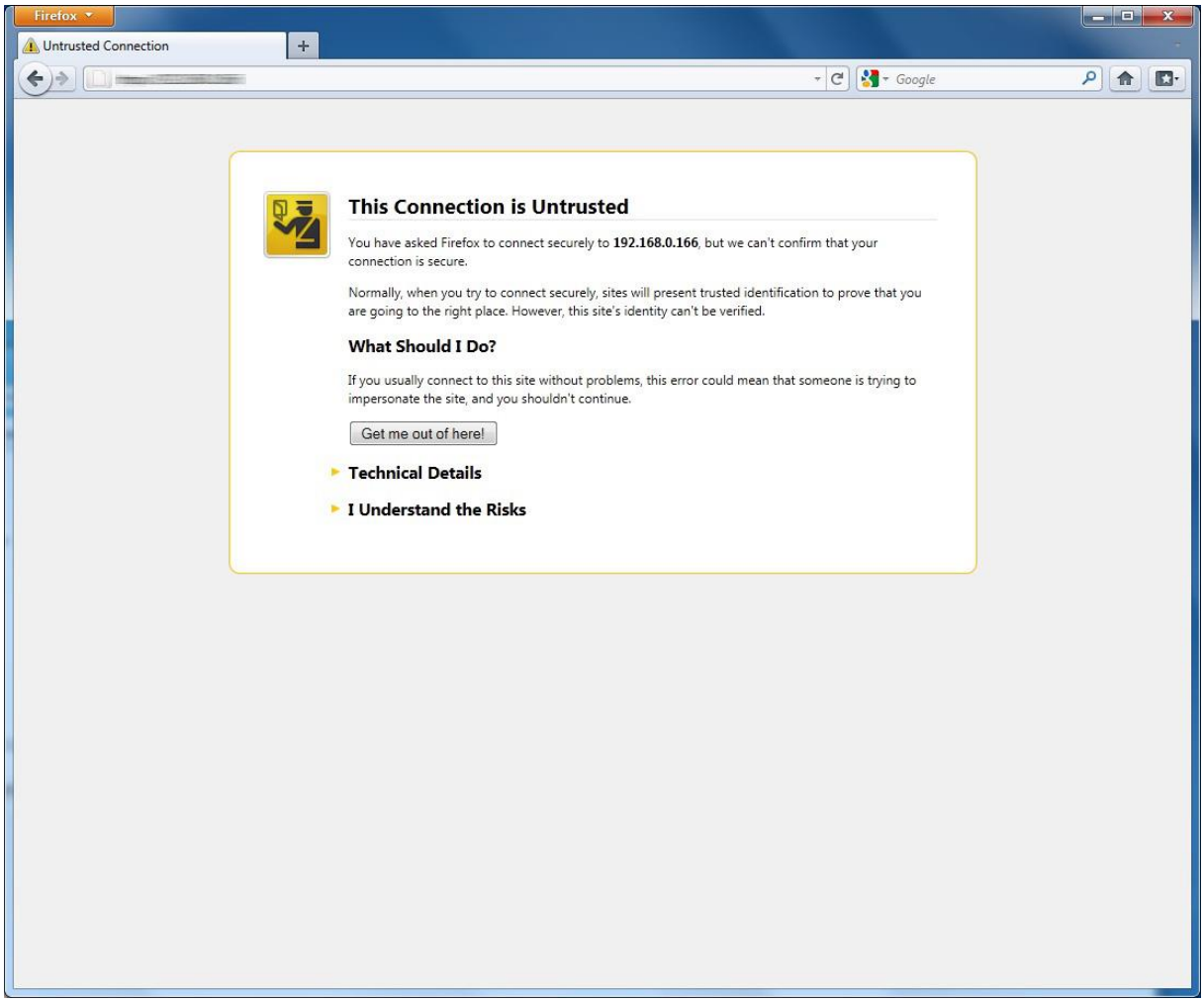
Close the Internet Explorer browser and try accessing the Endpoint Protector Administration and Reporting Tool IP address again.



18.2. For Mozilla Firefox

Open the Browser.

Open Endpoint Protector Administration and Reporting Tool IP address. (Your Appliance static IP Address, example https://192.168.0.201).


Firefox
Untrusted Connection
Google
This Connection is Untrusted
You have asked Firefox to connect securely to 192.168.0.166, but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
Get me out of here!
Technical Details
I Understand the Risks

From the above screenshot This Connection is Untrusted, choose I Understand the Risks. Click Add Exception.

Security Warning window pops up.

Just click Get Certificate button and then the Confirm Security Exception button.

Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location:
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View...
Wrong Site
Certificate belongs to a different site, which could indicate an identity theft.
Unknown Identity
Certificate is not trusted, because it hasn't been verified by a recognized authority.
Permanently store this exception
Confirm Security Exception
Cancel

Close and restart the browser.

19. Terms and Definitions

Here you can find a list of terms and definitions that are encountered throughout the user manual.

19.1. Server Related

Appliance – Appliance refers to the Endpoint Protector Appliance which is running the Endpoint Protector Server, Operating System, Databases, etc.

Computers – refers to PC's, workstations, thin clients, notebooks which have Endpoint Protector Client installed.

File Tracing - this feature will track all data that was copied to and from prior authorized portable storage devices.

File Shadowing – this feature saves a copy of all, even deleted files that were used in connection with controlled devices on a network storage server.

Devices – refers to a list of known portable storage devices, ranging from USB storage devices to digital cameras, LTP storage devices and biometric devices.

Groups – can be groups of devices, users or computers. Grouping any of these items will significantly help the server administrators to easily manage rights and settings for them.

Departments – an alternative way to Groups to organize main entities (devices, users or computers), which involves also the administrators of Endpoint Protector.

19.2. Client Related

Endpoint – can be a Personal Computer, a Workstation you use at the office or a Notebook. An endpoint can call and be called. It generates and terminates the information stream.

Trusted Devices – portable storage devices that carry a seal of approval from the Endpoint Protector Server and can be utilized according to their level (1-4). For more information please see "Enforced Encryption with Trusted Devices" section.

Client - refers to the client user who is logged in on a computer and who facilitates the transaction of data.

Rights – applies to computers, devices, groups, users and global rights; it stands for privileges that any of these items may or may not possess.

Online computers – refers to PC's, Workstations and/or Notebooks which have Endpoint Protector Client installed and are currently running and are connected to the Endpoint Protector server.

Connected devices – are devices which are connected to online computers.

Events – are a list of actions that hold major significance in Endpoint Protector. There are currently 17 events that are monitored by Endpoint Protector:

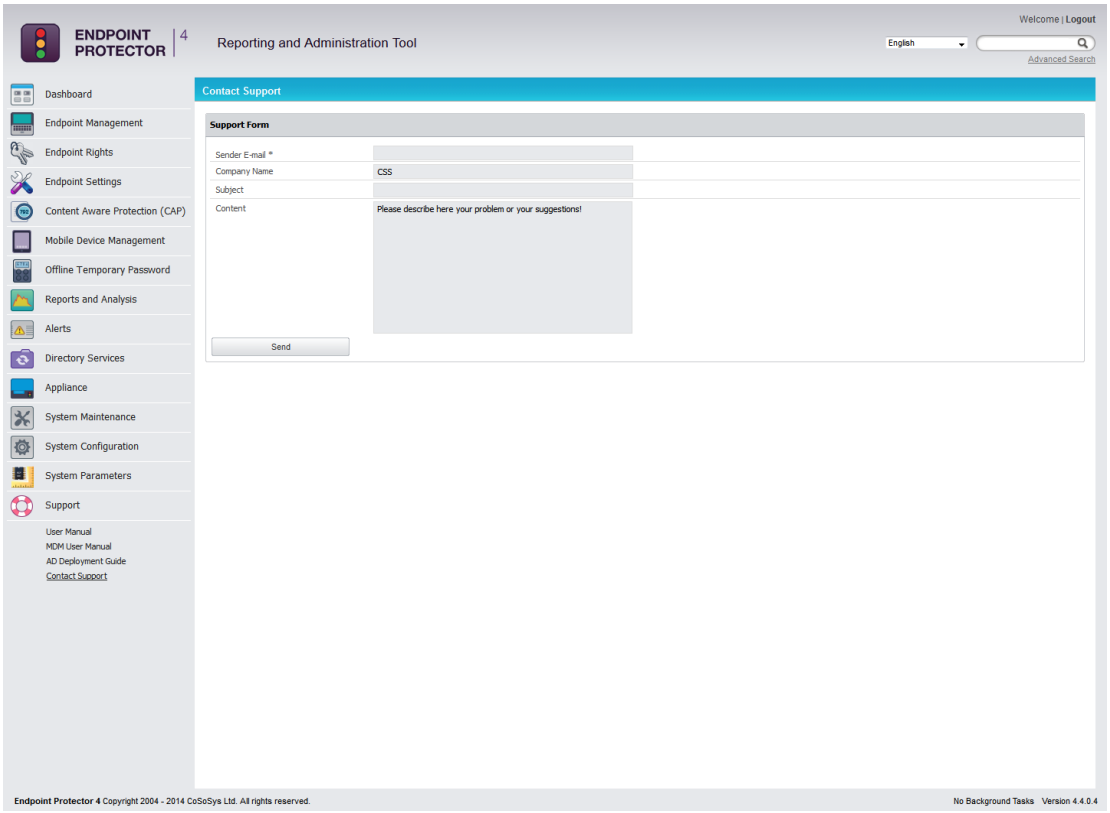
- Connected – the action of connecting a device to a computer running Endpoint Protector Client.
- Disconnected – the action of (safely) removing a device from a computer running Endpoint Protector Client.
- Enabled – refers to devices; the action of allowing a device access on the specified computer(s), group(s) or under the specified user(s).
- Disabled – refers to devices; the action of removing all rights from the device, making it inaccessible and therefore unusable.
- File read - a file located on a portable device was opened by a user or the file was automatically opened if the portable device was autorun by the operating system.
- File copy – a file was copied onto or from a portable device.
- File write – a file located on a portable device was opened and edited; changes were saved to the file.
- File renamed – a file located on a portable device has been renamed.

- File delete – a file located on a portable device has been deleted.
- Device TD – means that a device is registered as a Trusted Device and has access to files accordingly
- Device not TD – means that a device is not trusted and does not have automatic access to files
- Delete – refers to computers, users, groups, alerts and devices; the action of removing any of these items from the list
- Enable read-only – refers to devices; the action of allowing access to devices but disabling the ability to write on them. User(s) can copy files from device(s) but cannot write anything onto the device.
- Enable if TD Level 1-4 – refers to Trusted Devices; grants the device access if the device is a level one, two, three or four Trusted Device.
- Offline Temporary Password used – refers to computers, the action of temporarily allowing access to a specific device on a certain client computer.

20. Support

In case additional help, such as the FAQs or E-MAIL support is required, please visit our support website directly at http://www.cososys.com/help.html.

You can also write an E-MAIL to our Support Department under the Contact Us tab from the Support module.



One of our team members will contact you in the shortest time possible.

Even if you do not have a problem but miss some feature or just want to leave us general comment we would love to hear from you. Your input is much appreciated and we welcome any input to make computing with portable devices safe and convenient.

21. Important Notice / Disclaimer

Each Endpoint Protector Server has the default SSH Protocol (22) open for Support Interventions and there is one (1) System Account enabled (epproot) protected with a password. The SSH Service can be disabled at customers' request.

Security safeguards, by their nature, are capable of circumvention. CoSoSys cannot, and does not, guarantee that data or devices will not be accessed by unauthorized persons, and CoSoSys disclaims any warranties to that effect to the fullest extent permitted by law.

© 2004 – 2014 CoSoSys Ltd.; Endpoint Protector Basic, EPPBasic, Endpoint Protector, My Endpoint Protector are trademarks of CoSoSys Ltd. All rights reserved. Windows is registered trademark of Microsoft Corporation. Macintosh, Mac OS X are trademarks of Apple Corporation. All other names and trademarks are property of their respective owners.